02 2003
PC Games Hardware
TESTS TIPPS TUNING
DAS HARDWARE-MAGAZIN FÜR PC-SPIELER
Österreich € 6,90 Schweiz sfr 12,70 Dänemark dkr 55,- Italien/Spanien/Portugal/Frankreich/Griechenland € 8,10 Holland/Belgien/Luxemburg € 7,40
€ 6,50

SONDERAUSGABE

4 GIGABYTE SECURITY-TOOLS + TREIBER UND TRIAL-VERSIONEN AUF DVD-ROM!

Jeder PC ist in Gefahr!

Endlich Schutz vor: SPAM, VIREN & DIALERN

So stopfen Sie jedes Sicherheits-Loch!

Internet sicher
- 0190-Dialer abwehren
- Sicher vor Trojanern
- Outlook verriegeln

Daten schützen
- Sicherheitslücken unter Windows XP schließen
- Firewall optimal einsetzen

DVD

4,7 GIGABYTE SOFTWARE
Lebenswichtige Tools & Treiber griffbereit!

0190 Warner
Schutz vor Dialern

Endlich sicher vor der Gebührenfalle aus dem Internet!

Trojan Remover
30-Tage-Trial-Version

Der Rettungsanker, wenn ein Trojaner Ihren PC angreift!

Zone Alarm
Die kostenlose Firewall

Der zuverlässige Allround-Schutz gegen Attacken auf Ihren Computer!

Antivir
Personal Edition

Viren auf Ihrem PC aufspüren und ihnen den Garaus machen!

02
4 195756 806504

Seid Netz miteinander!

Stell Dir einfach eine Mischung aus Mixer, Toaster und Mikrowelle vor... :-) Tom !?

...Du meinst wohl den MicroLink-ADSL-Modem-Router-Switch ?!!

CeBIT
HANNOVER
12. – 19. 3. 2003

Besuchen Sie uns in
Halle 15, Stand C 34

MicroLink™ ADSL Modem Router
€ 199,90*
* unverbindl. Preisempfehlung

Tolle Mischung: 3 in 1 für alle ;-)))

Der MicroLink™ ADSL Modem Router: Die richtige Mischung aus ADSL-Modem, Router und 4-Port-Switch – mehrere PCs können direkt eine DSL-Leitung gemeinsam nutzen. Ideal geeignet für nette Wohngemeinschaften, grosse Familien oder kleine Büros. Einfach mit dem DSL-Splitter verbinden, PCs mit dem MicroLink™ ADSL Modem Router verbinden, konfigurieren – fertig!

- Highspeed-ADSL-Modem, Router und 4-Port-Switch in einem Gerät
- 4 PCs können direkt angeschlossen werden und über eine ADSL Leitung surfen (max. bis zu 253 PCs)
- Integrierte Firewall schützt vor Angriffen aus dem Internet
- Sehr einfache Installation, deutsche Konfiguration

Infos unter: Tel. +49 (0)241/182 79-79, info@devolo.de, www.devolo.de

devolo-Produkte sind erhältlich im gut sortierten Handel sowie bei Karstadt, Schauland, PC Spezialist, RED ZAC, Electronic Partner, amazon, Fröschl, Masters, MediMax und bei www.ep-netshop.de/partner/devolo.html

devolo-Produkte werden in Deutschland entwickelt!

devolo

devolo AG, Sonnenweg 11, 52070 Aachen

Analoge Modems | Industriemodems | ADSL-Modems | Router & Switches | Netzwerkadapter

Sicher durchs Netz

Internet-Wurm per E-Mail, Dialer beim Surfen und Trojaner durch Installation eines Tools aus dem Netz. Damit ist jetzt Schluss! Machen Sie Ihren PC so sicher wie eine Festung – das nötige Know-how bekommen Sie von uns.

FRANK NEUPERT
VERANTWORTLICHER REDAKTEUR
PC GAMES HARDWARE SONDERHEFTE

Können Sie sich vorstellen, endlich mal ganz entspannt im Internet zu surfen, Programme herunterzuladen und E-Mails zu öffnen? Die beunruhigende Entwicklung der Cyber-Kriminalität in den letzten Jahren lässt diesen einfachen Wunsch beinahe zu einer Utopie werden. Doch es gibt Mittel und Wege, wie Sie sich vor den meisten Gefahren aus dem Netz schützen können. Unsere aktuelle Sonderausgabe hilft Ihnen dabei, Ihren PC rundherum sicher zu machen.

Was hat man nicht schon alles über die ominösen Computerviren gehört. Kaum jemand kennt aber ihre Entstehungsgeschichte und weiß, wie sie eigentlich funktionieren. Wir bringen Licht ins Dunkel und stellen Ihnen verschiedene Arten von Viren vor. Wir versorgen Sie in unserem großen Wissens-Teil nicht nur mit wertvollem Hintergrundwissen zu Würmern, Trojanern, 0190-Dialern und anderen Schädlingen, sondern zeigen Ihnen auch, wie Sie sich wirksam davor schützen. In unserem Praxis-Teil unterziehen wir Windows XP und Outlook Express zudem einem ausführlichen Sicherheits-Tuning. Da das Thema Sicherheit nicht warten kann, haben wir die hervorragende Firewall Zone Alarm und den kostenlosen Virenscanner Antivir gleich mit auf unsere Heft-DVD gepackt!

Viel Spaß mit dem Sonderheft
wünscht Ihnen ...

PC Games Hardware gibt es auch als monatliches Hardware-Magazin.

Ausgabe 04/03 ist ab dem
05. März

bei jedem gut sortierten Zeitschriften-Händler erhältlich.

Wissen-Special:
0190-Dialer abgewehrt

SEITE 28

Schluss mit der Gebührenfalle:
Geben Sie 0190-Dialern keine Chance, sich an Ihnen eine goldene Nase zu verdienen! Unser Artikel klärt auf.

Praxis-Special:
Schutz durch Firewall

SEITE 52

Zone Alarm optimal einrichten:
Mit den richtigen Einstellungen bietet die kostenlose Firewall Zone Alarm optimalen Schutz für Ihren PC.

Software-Special:
Sicherheits-Tools

SEITE 70

Wie gut ist aktuelle Sicherheitssoftware?
In unserem Software-Test haben wir acht Sicherheits-Tools für Sie getestet. Darunter Virenscanner und Firewalls.

INHALT

Rubriken

3 Editorial
4 Inhalt Heft
5 Impressum

Wissen

6 Evolution der Viren
Was sind Computerviren und wo kommen sie her? Erfahren Sie alles über die Entstehungsgeschichte der digitalen Schädlinge.

10 Ihr Computer ist in Gefahr!
Ob Websites, E-Mails oder Software aus dem Netz: Potenzielle Gefahren lauern überall! Welche das sind, erfahren Sie hier.

14 Hacker-Tricks aufgedeckt
Hacker sorgen immer wieder für Verunsicherung und Ärger. Doch mit welchen teilweise banalen Tricks sie vorgehen, ist meist unbekannt.

18 Gefahr durch die Hintertür
Trojaner senden unbemerkt persönliche Daten an einen unbekannten Nutzer irgendwo im Netz. Lassen Sie es so weit erst gar nicht kommen!

22 Vorsicht, Spion an Bord!
Mit Spionage-Programmen wird die Schreckensvision vom gläsernen Nutzer immer realer. Wir zeigen, wie Sie Ihre Privatsphäre bewahren.

24 Makroviren attackieren Dokumente
Makroviren sind in der Lage, Ihre wertvollen Word- und Excel-Dokumente zu infizieren. Lesen Sie hier, wie Sie Ihre Dokumente schützen.

28 Schluss mit der 0190-Abzocke!
Astronomische Telefonrechnungen für nie genutzte Dienstleistungen, Ärger mit dubiosen Anbietern: So gehen Sie keinem Dialer mehr auf den Leim.

Praxis

34 PC sicher in null Komma nix
Sicherheit duldet keinen Aufschub! In diesem Praxis-Special erfahren Sie auf wenigen Seiten, wie Sie Ihren PC gegen alle Gefahren aus dem Netz wappnen.

46 Windows XP – aber sicher!
Essenzielle Tipps und Tricks auf fünf Seiten, wie Sie unter Microsofts aktuellem Betriebssystem Windows XP sämtliche Sicherheitslücken schließen.

52 Abgeschirmt mit Zone Alarm
Der ultimative Schutzschild für Ihren PC. Hier zeigen wir Ihnen, wie Sie die kostenlose Firewall so einrichten, dass sie optimalen Schutz bietet.

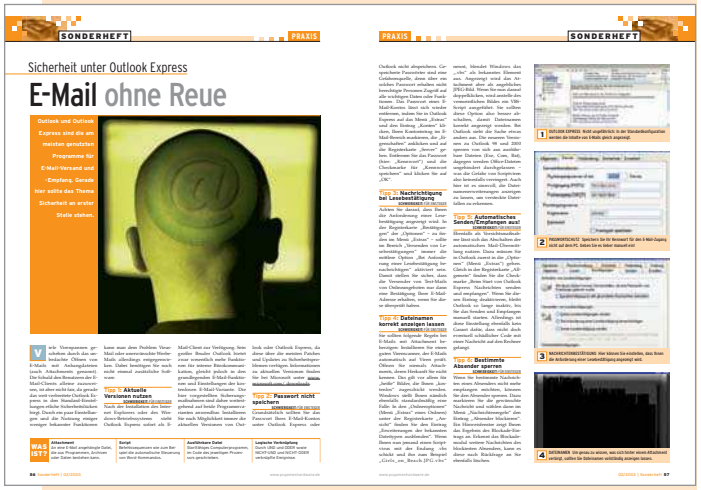
56 Outlook endlich sicher vor Spam und Viren
Spam, Viren, Kettenbriefe: Welche Einstellungen Sie unter Outlook vornehmen müssen, um sich davor zu schützen, verraten wir in diesem Teil.

60 Hacker im Visier
Ist Ihr PC schon mal Opfer eines Hacker-Angriffs geworden? Wie Sie sich am besten zur Wehr setzen und sich vor Angriffen schützen, lesen Sie hier.

Software

70 Sicherheits-Software im Test
Wir haben für Sie eine große Auswahl von Sicherheits-Software auf Herz und Nieren getestet. Die Ergebnisse stellen wir Ihnen hier vor.

Endlich Schluss mit Spam:
Outlook sicher

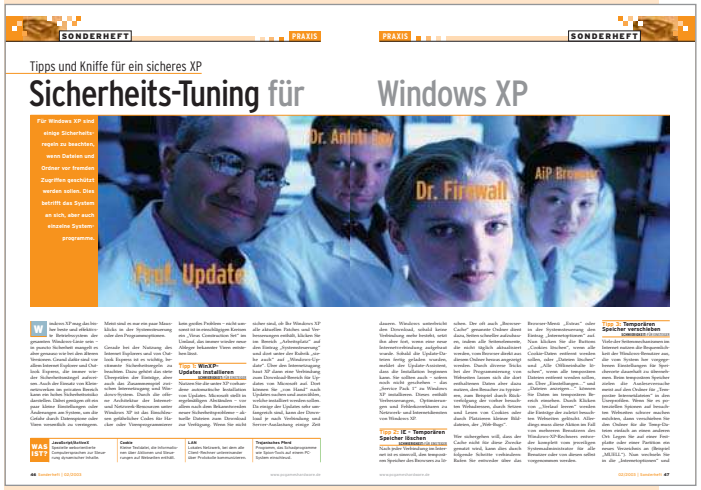


Seite 56

Optimale Einstellungen bei Outlook

Sie bekommen gerne E-Mails? Dann sorgt dieser Artikel dafür, dass es auch so bleibt! Sperren Sie Spam, Viren und Kettenbriefe zuverlässig aus.

Gefahren abwehren:
XP verriegelt



Seite 46

Sicherheits-Tuning für XP:

In unserem umfangreichen Praxis-Artikel zeigen wir Ihnen, wie Sie Sicherheitslücken schließen und Ihr Betriebssystem vor fremden Zugriffen schützen.

Impressum

[ANSCHRIFT DER REDAKTION]
COMPUTEC MEDIA AG
PC Games Hardware
Dr.-Mack-Straße 77, 90762 Fürth

E-Mail:
redaktion@pcgameshardware.de
Fax: 0911/28 72 - 200

Vorstand:
Christian Geltenpoth (Vorsitzender),
Niels Herrmann, Oliver Menne

Chefredaktion:
Thilo Bayer (*tb*) (V. i. S. d. P.)

Verantwortlicher Redakteur Sonderhefte:
Frank Neupert (*fn*)

Mitarbeiter dieser Ausgabe:
Marco Albert (*ma*), Jürgen Borngießer (*jb*), Christian Gögelein (*cg*), Frank Mischkowski (*fm*), Jivko Seizov (*js*)

Textchef: Michael Ploog,
Margit Koch-Weiß (Stellvertretung)

Lektorat: Birgit Bauer,
Claudia Brose, Esther Marsch, Cornelia Lutz

Redaktion Cover-CD-ROM:
Jürgen Melzer (Leitung), Jasmin Sen

Layout:
Simon Schmid, Marco Leibetseder,
Hans Strobel

Titelgestaltung & Grafische Konzeption:
Simon Schmid

Bildredaktion: Albert Kraus

Art Director: Andreas Schulz

[ANZEIGENKONTAKT]
COMPUTEC MEDIA SERVICES GmbH
Dr.-Mack-Straße 77
90762 Fürth

Telefon: +49 - 911/28 72 - 341
Fax: +49 - 911/28 72 - 241
E-Mail: jasmin.zemsch@computec.de

Anzeigenleitung:
Thorsten Szameitat
E-Mail: thorsten.szameitat@computec.de

Anzeigenberatung:
Wolfgang Menne (V. i. S. d. P.)
Fax.: +49 - 911/28 18 - 244
E-Mail: wolfgang.menne@computec.de

Anzeigendisposition:
Andreas Klopfer
E-Mail: andreas.klopfer@computec.de

Anca Stef
E-Mail: anca.stef@computec.de

Datenübertragung:
ISDN PC: +49 - 911/28 72 - 261
ISDN Mac: +49 - 911/28 72 - 260

[VERLAG]
COMPUTEC MEDIA AG
Dr.-Mack-Straße 77,
90762 Fürth

Produktion:
Ralf Kutzer (Leitung)

Vertriebsleitung:
Klaus-Peter Ritter

Werbeabteilung:
Martin Reimann (Leitung),
Jeanette Haag

[VERTRIEB]
Burda Medien Vertrieb

[ABONNEMENT]
PC Games Hardware kostet im Abonnement mit CD-ROM € 43,20 für 12 Ausgaben
Im Ausland außer Österreich € 56,40
Österreich: € 50,20

Kundenservice (Inland und Ausland außer Österreich):
Computec Abo-Service
Postfach 1129, 23612 Stockelsdorf

Tel.: (0451) 49 06 - 700
Fax: (0451) 49 06 - 770
E-Mail: computec.abo@pvz.de

Abonnement Österreich:
Leserservice GmbH
St. Leonharder Straße 10
A-5081 Anif
Tel.: 06246/882 - 882
Fax: 06246/882 - 5277
E-Mail: bgenser@leserservice.at

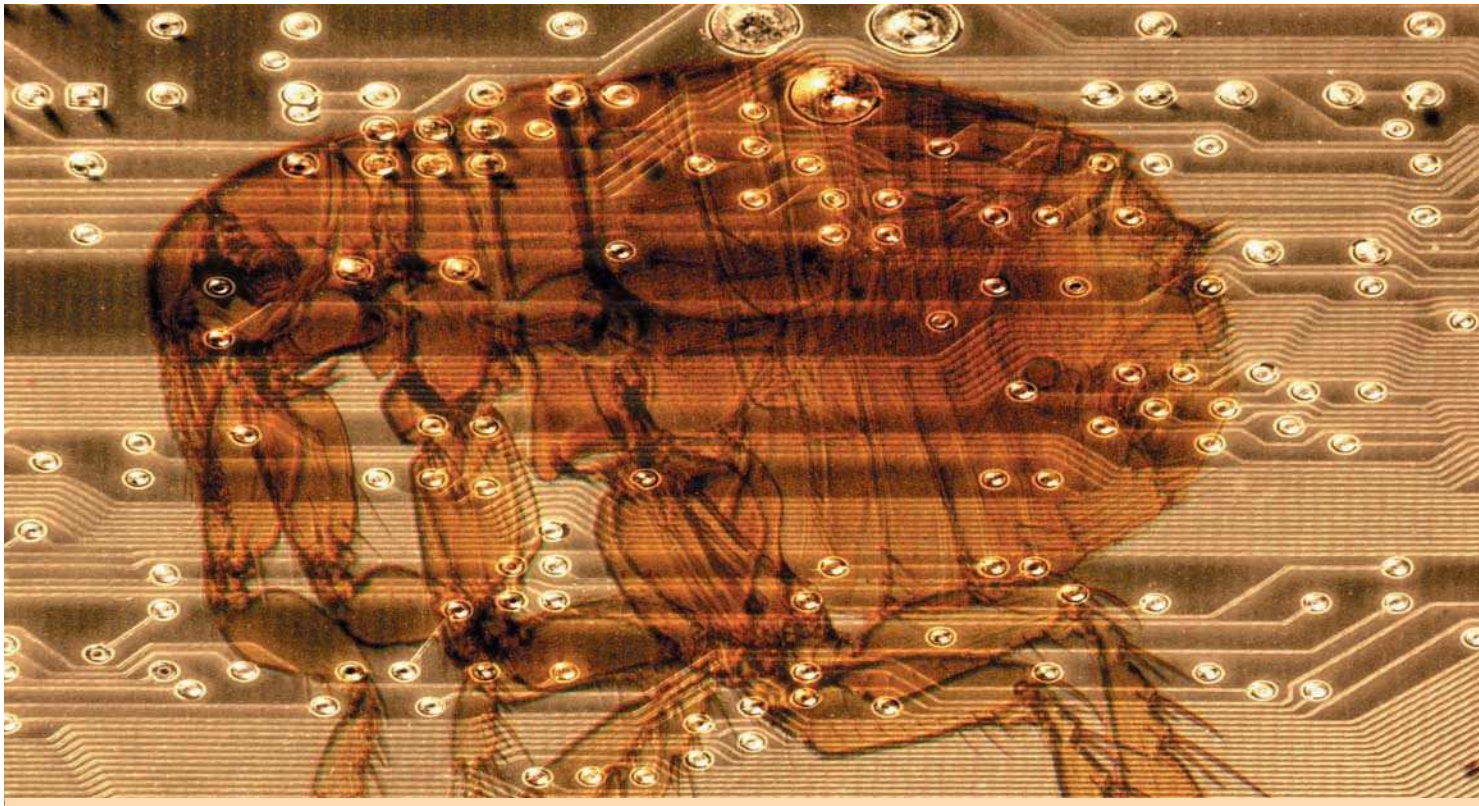
ISSN/Pressepost:
PC Games Hardware wurden folgende ISSN- und Postvertriebsnummern zugeteilt:
VKZ: B 53384 | ISSN:1616-6922

[DRUCK]
Oberndorfer Druckerei GmbH;
A-5110 Oberndorf bei Salzburg

Mitglied der Informationsgemeinschaft zur Feststellung der Verbreitung von Werbeträgern e. V. (IVW), Bad Godesberg:

Verbreitete Auflage,
I. Quartal 2003:
85.545 Exemplare

Manuskripte und Programme: Mit der Einsendung von Manuskripten jeder Art gibt der Verfasser die Zustimmung zur Veröffentlichung in den von der Verlagsgruppe herausgegebenen Publikationen.
Urheberrecht: Alle in PC Games Hardware veröffentlichten Beiträge bzw. Datenträger sind urheberrechtlich geschützt. Jegliche Reproduktion oder Nutzung bedarf der vorherigen ausdrücklichen und schriftlichen Genehmigung des Verlages. Die Benutzung und Installation der Datenträger erfolgt auf eigene Gefahr. Der Verlag übernimmt für Fehler, die durch die Benutzung der auf den Datenträgern enthaltenen Programme entstehen, keine Haftung. Die Programme stellen keine Entwicklung des Verlages dar, sondern sind Eigentum des Herstellers. Für den Inhalt der Programme sind die Autoren verantwortlich. COMPUTEC MEDIA ist nicht verantwortlich für die inhaltliche Richtigkeit der Anzeigen und übernimmt keinerlei Verantwortung für in Anzeigen dargestellte Produkte und Dienstleistungen. Die Veröffentlichung von Anzeigen setzt nicht die Billigung der angebotenen Produkte und Service-Leistungen durch COMPUTEC MEDIA voraus. Sollten Sie Beschwerden zu einem unserer Anzeigenkunden, seinen Produkten oder Dienstleistungen haben, bitten wir Sie, uns dies schriftlich mitzuteilen. Schreiben Sie unter Angabe des Magazins inkl. der Ausgabe und der Seitennummer, in dem die Anzeige erschienen ist, an: COMPUTEC MEDIA SERVICES GmbH, Anschrift siehe oben.



Geschichte der Computerviren

Evolution digitaler

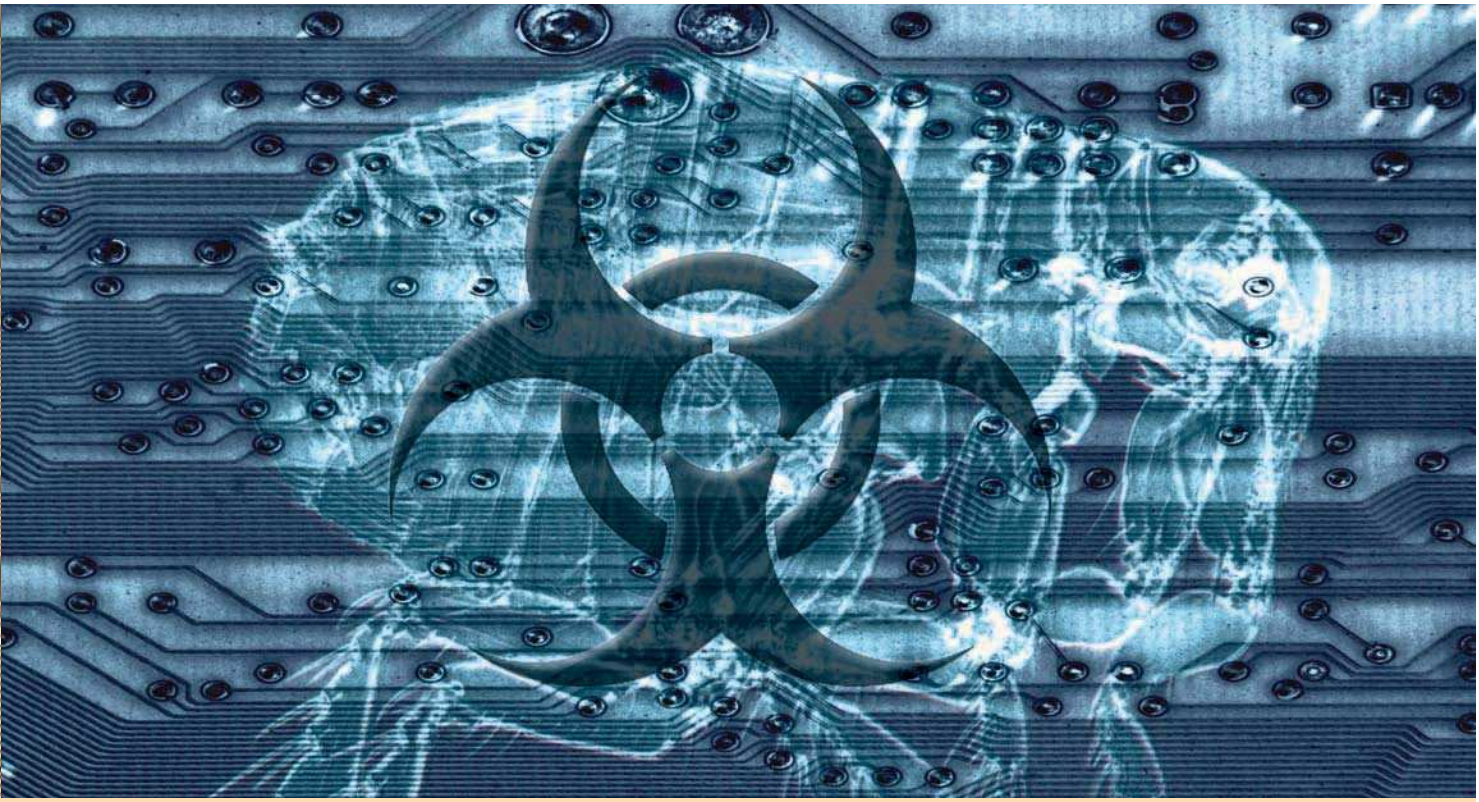
Computerviren sind zu einer Plage geworden. Trotz mittlerweile weit verbreiteter Antiviren-Software verursachen sie weltweit immer noch enorme Schäden. Doch was genau sind Viren und wie sind sie entstanden?

Durch entsprechende Meldungen in der Presse gelangen Computerviren immer wieder zu zweifelhafter Berühmtheit. Kein Wunder, schließlich haben „I LOVE YOU“ und „Melissa“ der weltweiten Wirtschaft Verluste in Millionenhöhe „beschert“. Aber auch ihre weniger bekannten Artgenossen sorgen in Privathaushalten und Büros immer wieder für Ärger und zusätzliche Arbeit. Ein großes Problem ist nicht nur die rasche Verbreitung der Viren, sondern auch die immer neuen Ansätze ihrer Programmierer. So liegt es in der Natur der Sache, dass Antiviren-Software eigentlich nie auf dem aktuellsten Stand sein kann, da immer irgendwo irgendjemand über einer neuen, bis dato unbekannten Viren-Form brütet. Natürlich haben sich auch Virenschutzprogramme im Laufe der Zeit weiterentwickelt und stellen daher eine durchaus adäquate Waffe im Kampf gegen die virtuellen Schädlinge dar – hundertprozentigen Schutz können aber auch sie nicht bieten. Ein brisantes Thema also, weshalb wir in diesem Artikel versuchen, das Phänomen „Computervirus“ ein wenig zu durchleuchten.

Was ist ein „Computervirus“?

SCHWIERIGKEIT: FÜR EINSTEIGER

Auf technischer Ebene betrachtet ist ein Virus ein ausführbares Programm („Code“) von meist geringer Größe. Computerviren entstehen nicht einfach, sondern werden mit einer bestimmten Absicht programmiert. Weshalb aber die Bezeichnung „Virus“? Um diese Frage zu beantworten, ziehen wir zunächst einmal die Biologie zu Rate: Viren dringen in die Wirtszellen des menschlichen Körpers ein und verändern deren Informationen so, dass diese Zellen von nun an auch den Virus produzieren – der Virus vervielfältigt sich also. Dieser Vorgang bleibt für den Organismus nicht ohne Folgen: Man wird krank und steckt überdies auch noch seine Mitmenschen an. Kurz gesagt gibt es bei biologischen Viren zwei wichtige Eigenschaften: die Fähigkeit, sich selbst zu reproduzieren (und zu verbreiten) und Schaden anzurichten. Bei Computerviren passiert etwas ganz Ähnliches. Die kleinen Programme werden vom Programmierer in ein beliebiges Wirtsprogramm eingesetzt. Bei Aufruf dieses Wirtes – zum Beispiel einer Textdatei – wird der Virus aktiviert und sucht sich mindestens ein weiteres Programm, das er ebenfalls infiziert. Oft werden infizierte Programme dabei überschrieben und damit zerstört. Der Virus vervielfältigt sich nicht nur auf einem lokalen System, sondern auch in Netzwerken und über Datenträger (zum Beispiel Disketten oder Wechselplatten), wodurch also auch andere Rechner „angesteckt“ werden. Wie ihre biologischen Vorbilder haben auch Virenprogramme diese zwei Komponenten: zum einen den Verbreitungsmechanismus des Virus, der bewirkt, dass er sich selbst in andere Programmdateien hineinkopiert und sich sys-



Schädlinge

tematisch von einer Datei zur anderen, von einem Rechner zum anderen ausbreitet, zum anderen die Nutzlast oder Schadensroutine – also die Programmkomponente, die bestimmte Symptome oder Schäden am infizierten Rechner hervorruft. Computerviren können nach Art der Schadensroutine in „gutartig" und „bösartig" unterteilt werden. Gutartige Viren werden lediglich zu dem Zweck entwickelt, den Benutzer zu ärgern (beispielsweise mit nervenden Meldungen auf dem Bildschirm) und nicht, um den Computer zu beschädigen. Bösartige Viren hingegen werden mit der Absicht programmiert, dem Wirtsrechner Schaden zuzufügen, der von der Datenzerstörung bis zur totalen Lahmlegung des Systems führen kann. Aber wie sind Viren eigentlich entstanden?

Von der Idee zu den ersten Versuchen

SCHWIERIGKEIT: FÜR EINSTEIGER

Die Theorie des Virus geht bis ins Jahr 1949 zurück, wenngleich damals noch niemand an solche Programme dachte: In diesem Jahr entwickelte der ungarische Informatiker John von Neumann (1903-1957) die Theorie der sich selbst reproduzierenden Automaten. Seine Idee war folgende: Programme und Daten sollten in einem gemeinsamen Speicher verstaut werden – vorher waren diese Komponenten noch getrennt. Das bedeutet, dass das Rechenwerk (die CPU) Befehle genauso wie Daten behandelt. Dahinter verbirgt sich bereits das Grundkonzept des Computervirus. Schließlich sind Viren ja nichts anderes als Programme, die sich selbst und andere wie Daten behandeln, verarbeiten, verändern und infizieren. Gut 20 Jahre später leisteten Mitarbeiter der Bell Laboratories einen wichtigen Beitrag zur Entstehung des Virus: Sie entwickelten ein Computerspiel namens *Darwin*. Bei diesem Spiel „bekämpfen" sich zwei oder mehrere Programme im Speicherbereich eines Computers. Mehrere Programme wetteifern darum, dem jeweils anderen Programm Rechenleistung zu stehlen oder es zu zerstören. Je geschickter ein Programmierer sein Programm gestaltet hat, umso größer sind seine Überlebenschancen. Bekannt wurde *Darwin* 1984 unter dem neuen Namen *Core Wars* (zu Deutsch „Kernkriege"), weil sich der „Kampf" vor allem im Computerspeicher (Kern) abspielte. Von Experten wird *Core Wars* übrigens als erster Computerwurm der Geschichte bezeichnet. Selbstständig verbreiten konnte er sich allerdings noch nicht, hierfür war er auf die Hilfe der Programmierer angewiesen.

Der erste funktionsfähige Virus

SCHWIERIGKEIT: FÜR FORTGESCHRITTENE

Den Begriff „Computervirus" führte 1981 Professor Len Adleman ein. Er gebrauchte diesen Begriff während eines Gesprächs mit seinem Doktoranten Fred Cohen. Cohen war es dann auch, der zwei Jahre später den ersten funktionsfähigen Virus vorstellte. Er wurde unter UNIX programmiert und nistete sich in einem bestimmten Befehl ein. Jedes Mal, wenn der Virus zur Ausführung kam, „erbte" er die Systemprivilegien des infizierten Programms und konnte so innerhalb kürzester Zeit jedem Benutzer diese Privilegien übertragen. Dieser und andere expe-

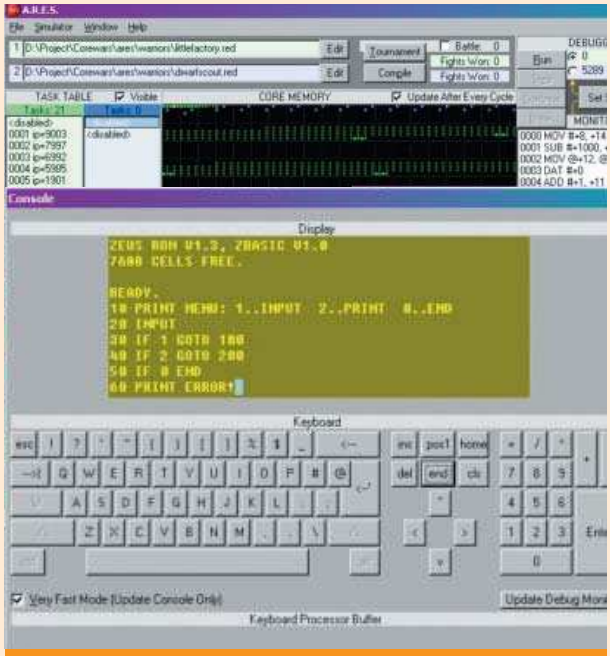
Geschichte des Schreckens

Was mit einer Idee begann und mit einem Spiel weiterging, mündete später in eine Plage: Computerviren.

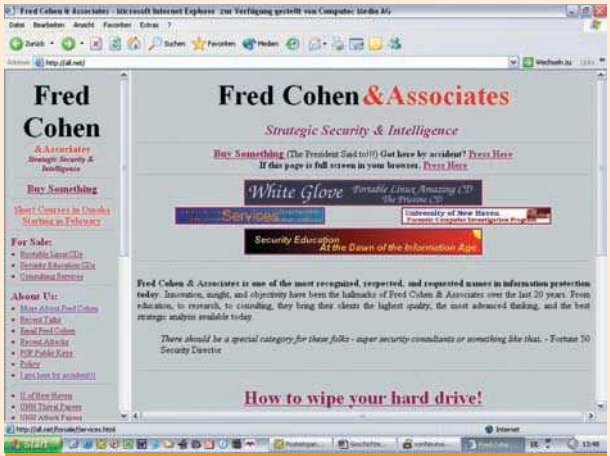
Chronologie

Zeitpunkt	Ereignis
1949	Der ungarische Informatiker John von Neumann entwickelt die Theorie der sich selbst reproduzierenden Automaten und schuf damit das Grundkonzept, das sich hinter Computerviren verbirgt.
1962-1984	Drei Mitarbeiter der Bell Labs programmieren das Computerspiel *Core Wars* (vorher *Darwin*). Bei dem Spiel „bekämpfen" sich zwei oder mehr Programme im Speicherbereich eines Computers. *Core Wars* gilt als Vorläufer des Computervirus.
1981	Professor Len Adleman erfindet den Begriff „Computervirus".
1982	Fred Cohen stellt im Rahmen seiner Doktorarbeit den ersten lauffähigen Virus für die UNIX-Plattform vor.
1986	Zwei pakistanische Brüder programmieren den ersten MS-DOS-Virus und bringen ihn über Disketten in weltweiten Umlauf.
1987	Erster großer Virenboom: Bootsektorenviren überschwemmen die Computerwelt. McAfee bringt seinen ersten Virenscanner heraus.
1988	Der erste Internetwurm legt 6.000 Server in den USA lahm.
Ab 1990	Die ersten intelligenten, so genannten „polymorphen" Viren treten auf den Plan.
1995	Makroviren erobern die Welt. Word- und Excel-Dokumente sind von nun an nicht mehr sicher.
1996	Der erste Virus für Windows 95 taucht auf.

VISIONÄR Der ungarische Informatiker John von Neumann entwickelte bereits 1949 die Idee von sich selbst reproduzierenden Automaten.



KERN KRIEGE Das Spiel „Core Wars" gilt als Vorläufer des Computervirus: Mehrere Programme „bekämpfen" sich im Speicher eines Computers.



VATER ALLER VIREN? Fred Cohen entwickelte den ersten, funktionsfähigen Virus unter dem UNIX-System und ist heute Spezialist für IT-Sicherheit.

rimentelle Viren waren Gegenstand von Cohens Doktorarbeit und somit einer breiten Öffentlichkeit zugänglich. Zwar galt seine Arbeit damals als umstritten, doch von da an fand eine rasante Entwicklung der Viren statt.

Erster MS-DOS-Virus geht um die Welt

SCHWIERIGKEIT: FÜR FORTGESCHRITTENE

Im Jahr 1986 kam der erste MS-DOS-Virus in Umlauf: „Pakistani Brain" verbreitete sich über Disketten, auf denen raubkopierte Software gespeichert war. Auf den infizierten Disketten markierte der Virus einen Teil der Floppy als beschädigt und versteckte seinen Code in diesen angeblich beschädigten Sektoren. Programmiert hatten den Erreger zwei 19 und 26 Jahre alte Brüder aus Lahore in Pakistan. Das Duo betrieb einen Shop für Raubkopien und verkaufte die illegale Software auf infizierten Disketten. Die Absicht der beiden war es, ihre Kunden auf diese Weise an ihren eigenen Service-Dienst zu binden. Der Virus forderte den Benutzer nämlich auf, die Diskette in den Laden zurückzubringen, um sie dort reparieren zu lassen. Das Erstaunen der Pakistani muss groß gewesen sein, als sie erfuhren, dass sich ihr Virus bis in die Vereinigten Staaten verbreitet hatte.

Der erste, große Virenboom

SCHWIERIGKEIT: FÜR EINSTEIGER

1987 kann man als Jahr des Virenbooms bezeichnen. An der Lehigh-Universität in den USA machte zum ersten Mal ein Virus von sich reden, der die DOS-Datei command.com infizierte. Der Virus machte es sich zunutze, dass jeder Aufruf in DOS über diesen Kommandozeileninterpreter abgewickelt wird, so dass der Virus ständig die Kontrolle behielt. Nach dem vierten Aufruf überschrieb der Schädling die Sektoren 1 bis 32 und meldete „Hasta la vista, Floppy" auf dem Schirm. Doch die Viren-Seuche nahm damit gerade mal ihren Anfang: Ganze Schwärme von Bootsektorenviren piesacken die Computerwelt mit teilweise recht obskuren Symptomen. Bei einem Erreger italienischer Herkunft hüpft dauernd ein Ball auf dem Bildschirm herum, ein Virus aus Neuseeland meldet sich mit „Your Computer is now stoned. Legalize marijuana.". Auch Dateiviren verbreiten sich in diesem Jahr zunehmend. Der dank Medienberichterstattung bekannteste

Vertreter seiner Art war „PLO“ beziehungsweise „Jerusalem“. An jedem Freitag den 13. löschte der Fiesling alle Dateien mit den Endungen „.com“ und „.exe“.

1987 war auch das Jahr, in dem McAfee seinen ersten Virenscanner herausbrachte, der damals sage und schreibe 19 verschiedene Viren erkennen konnte.

Erster Internetwurm legt Server lahm

SCHWIERIGKEIT: FÜR FORTGESCHRITTENE

Der erste Internet-Wurm debütierte im November 1988 und versetzte dem damals noch jungen Internet einen schweren Schlag. Der völlig unberechenbare Wurm infizierte innerhalb weniger Stunden Tausende von Internet-Systemen. Durch seine rasche Vermehrung und Verbreitung verschlang er so viel Rechenleistung, dass über 6.000 Computer in den USA nach kurzer Zeit lahm gelegt waren. Vielen Betreibern von Websites blieb als letzter Ausweg nur noch, den Netzstecker zu ziehen. Von diesem Super-GAU erholte sich das weltweite Netz erst nach einigen Wochen. Pikantes Detail: Autor des Wurms war ein gewisser Robert T. Morris, Sohn des amerikanischen Sicherheitsspezialisten Robert Morris Sr., der bereits mit dem ersten experimentellen Virus in *Darwin* beziehungsweise *Core Wars* erste Erfahrungen mit dieser Technologie gemacht hatte.

Viren werden klug

SCHWIERIGKEIT: FÜR FORTGESCHRITTENE

In den 90ern erreichte die Evolution der Viren einen neuen Höhepunkt: Computerviren bekamen von ihren Schöpfern eine Art künstliche Intelligenz und verhielten sich von nun an fast so wie ihre in der Natur vorkommenden Vorbilder: Sie verändern durch das Tauschen von Bytefolgen und Einfügen von Dummy-Codes ständig ihre Form. Diese Mutationen haben zur Folge, dass der Virus nach jedem Aufruf anders aussieht als vorher, weshalb man diese Viren-Typen auch als „polymorph“ (vielgestaltig) bezeichnet. Hersteller von Antiviren-Software hatten dieser neuen Virus-Form anfänglich wenig entgegenzusetzen, so dass eine ganze Armada von intelligenten Viren heranwachsen und sich vermehren konnte.

Makroviren greifen Dokumente an

SCHWIERIGKEIT: FÜR FORTGESCHRITTENE

Wer glaubte, Viren könnten keine Dokumente infizieren, wurde im August 1995 eines Besseren belehrt. Mitte der Achtzigerjahre orakelte Virenschutz-Pionier John McAfee: „Ich glaube, die Chance, dass so etwas passiert, ist etwa so groß, wie von einem Meteoriten getroffen zu werden“. Dann passierte es aber doch: „WinWord.Concept“ bildete die Vorhut für ein ganzes Heer von Makroviren und markierte einen Wendepunkt in der Virengeschichte. Von nun an terrorisierten hauptsächlich Makroviren die Computerwelt.

Makroviren setzen auf Microsofts Makrosprache in Word auf. Die Textverarbeitung führt beim Öffnen oder Schließen automatisch bestimmte Makros aus – ähnlich wie Programme im Autostart-Verzeichnis von Windows. Die Makros kopieren sich in die globale Dokumentenvorlage „normal.dot“. Da diese Vorlage beim Öffnen eines Dokumentes immer geladen wird, kopieren sich die Makros in jedes Dokument, das nach der Infektion geöffnet wird.

Der Anfang vom Ende?

SCHWIERIGKEIT: FÜR EINSTEIGER

1996 geschah dann das, womit eigentlich schon jeder gerechnet hatte: Es tauchte der erste Virus speziell für Windows 95 auf. Spätestens jetzt gehörten Viren zum Computer-Alltag: Jeder musste damit rechnen, sich zu „infizieren“. Diese Brisanz haben Viren bis heute behalten, wenngleich auch ein gewisses Bewusstsein gegenüber dieser Thematik gewachsen ist und ein guter Virenscanner heutzutage zur Standardausrüstung jedes PCs gehört. Dennoch: Stets neue und noch ausgefeiltere Ansätze seitens der Viren-Programmierer schaffen immer neue Gefahren, gegen die es noch keinen Schutz gibt. „Melissa“ und „I LOVE YOU“ aus jüngster Vergangenheit sollten uns diesbezüglich ausreichend gewarnt haben.

FRANK NEUPERT

INTERNET-WURM Seit 1988 grassieren immer wieder Meldungen über Würmer wie „I LOVE YOU“, die tausende von Systemen lahm legen.

MAKROVIRUS Der Makrovirus „Winword Concept“ bewies erstmalig, dass auch Dokumente von Viren infiziert werden können.

FUNDGRUBE Auf den Webseiten von F-Secure finden Sie detaillierte Informationen zu fast allen jemals in Erscheinung getretenen Viren.

VIRENSCANNER McAfee gehört zu den Pionieren im Kampf gegen Viren. Ein guter Virenscanner gehört heutzutage zu jedem PC dazu.

Sicherheitsrisiko Computer

Gefahren für Ihren PC

Nachdem Sie gerade etwas über die Entstehung von Viren erfahren haben, wird es Zeit, die tückischen Schädlinge etwas genauer zu beleuchten. Welche Arten von Viren gibt es? Und was können sie anrichten?

Da Viren grundsätzlich jedes Betriebssystem befallen können, sind auch alle Computerbesitzer von dieser Problematik betroffen. Zwar hört man immer wieder, dass es für Linux- und Macintosh-Rechner kaum Viren gibt – dennoch sollte auch hier die Gefahr nicht unterschätzt werden, wenngleich der Windows-PC nach wie vor das verbreitetste System bleibt und es demnach auch entsprechend viele Viren und Würmer gibt. Bei dieser Vielfalt ist schnell klar, dass Virus nicht gleich Virus ist: Sie lassen sich in verschiedene Klassen einteilen, haben unterschiedliche Wirkungsweisen – auch geht es nicht immer nur darum, destruktiven Schaden anzurichten. Mittlerweile werden die digitalen Eindringlinge auch zu Spionage und Datenraub eingesetzt.

Auf welche Weise verbreiten sich Viren?

SCHWIERIGKEIT: FÜR EINSTEIGER

Besonders gefährlich machen Viren die Fähigkeit, sich auf unterschiedlichste Weise zu vermehren und zu verbreiten. Ein einfacher und effizienter Weg sind Disketten und Wechselplatten, da diese oft mit anderen Benutzern getauscht werden und die Viren so ohne große Umwege von einem Opfer zum nächsten gelangen können. Eine andere Möglichkeit sind Netzwerke: Gerade heutzutage erfolgt der Datenaustausch immer mehr über lokale (LAN) und globale (WAN) Netzwerke. Viele moderne Viren verbreiten sich bevorzugt beim Daten- und Programmaustausch – hier dienen Programme und Dokumente als Wirte. Einige Viren gelangen durch die Verbreitung mittels E-Mail auf Millionen von Rechnern (zum Beispiel „I LOVE YOU"). Zwar kann sich im Text einer normalen E-Mail noch kein Virus befinden – dafür aber in den Attachments! Eine andere beliebte Art, Viren einzuschleusen, sind Internet-Downloads, weshalb hier besondere Vorsicht geboten sein sollte: In jeder heruntergeladenen Datei zweifelhafter Herkunft kann sich ein Virus verbergen. Überhaupt machen sich gerade in letzter Zeit immer mehr Schädlinge das Internet zunutze. Manche nisten sich direkt in HTML-Seiten ein. VB-Script, Java und vor allem ActiveX sind immer wieder beliebte Angriffsziele der Viren-Programmierer. Der Internet Explorer von Microsoft ist besonders anfällig für solche Virentypen. Programmfehler und Sicherheitslücken machen es den Schädlingen noch leichter. Wir empfehlen unbedingt, das Service Pack 1 zu installieren, da es bereits etliche Sicherheitslücken bei der Version 6 des Internet Explorers schließt.

Grüße aus Troja

SCHWIERIGKEIT: FÜR EINSTEIGER

Von so genannten Trojanischen Pferden, oder auch kurz Trojaner genannt, hört man in letzter Zeit immer öfter. Hierbei handelt es sich um Programme, die der Nutzer im guten Glauben installiert, dass es sich hierbei um ein hilfreiches Tool oder Spiel handelt. Wird die vermeintlich harmlose Applikation dann gestartet, aktiviert sich der Trojaner und der PC mit sämtlichen Daten ist von nun an nicht mehr sicher: Von Spionage über Datenraub bis hin zum Löschen aller auf der Festplatte befindlichen Daten – bei diesen perfiden Eindringlingen ist mit allem zu rechnen.

Spezielle Trojaner, so genannte Dropper, dienen auch als Träger von Viren, die ihre gefährliche Fracht in das System „droppen“, also einsetzen. Am besten schützen Sie sich, indem Sie möglichst alle Dateien unbekannter Herkunft, die zudem noch solch „verführerische“ Bezeichnungen wie „STARTME.EXE“ tragen, sofort löschen. Trojanische Pferde können sich im Gegensatz zu Viren und Würmern nicht von selbst fortpflanzen.

Angriff auf Dokumente – Makroviren

SCHWIERIGKEIT: FÜR EINSTEIGER

Makroviren sind eine Sonderform der Viren, die ausschließlich Dokumente befallen. Sie sind deshalb in der Lage, Dokumente zu infizieren, weil sie in der entsprechenden Makrosprache von zum Beispiel Win Word, Access, Excel oder Star Office entwickelt werden. Zwar können sich die Schädlinge nur dann verbreiten, wenn die entsprechenden Programme auch gestartet werden, doch gerade das Erstellen von Dokumenten ist ja eine der häufigsten Tätigkeiten am PC, weshalb eine Infektion mit einem Makrovirus normalerweise nie ohne Folgen bleibt. Makroviren können sich sogar plattformübergreifend ausbreiten wie beispielsweise MS-Word-Makroviren, da Word-Dateien sowohl auf einem Windows-PC als auch auf einem Apple Macintosh verarbeitet werden können.

Wenn da mal nicht der Wurm drin ist ...

SCHWIERIGKEIT: FÜR EINSTEIGER

Als Wurm wird ein Programm bezeichnet, das sich selber vervielfältigt, jedoch keinen Wirt infiziert. Würmer können also nicht Bestandteil anderer Programmabläufe werden. Viele Würmer haben lediglich den einen Zweck, sich so schnell wie möglich zu verbreiten. Je nachdem wie rechenintensiv dieser Prozess ist, können damit ganze Computersysteme lahm gelegt werden – was dann meist auch das Ziel der Wurm-Programmierer ist. Sie können aber auch Dateien umbenennen oder sogar löschen.

Echt komisch! Scherzprogramme

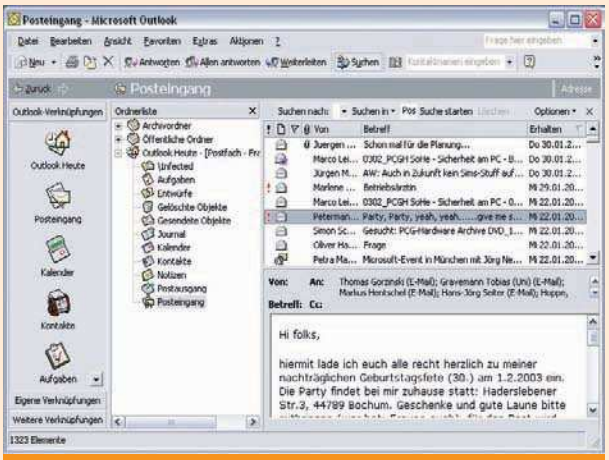
SCHWIERIGKEIT: FÜR EINSTEIGER

So genannte Witz- oder Scherzprogramme werden geschrieben, um jemanden einen Schrecken einzujagen oder zu ärgern. In den meisten Fällen richten sie keinen Schaden an und vermehren sich auch nicht – es sei denn, der Nutzer gibt sie absichtlich an andere weiter. Wie sich diese Witzprogramme bemerkbar machen ist ganz unterschiedlich: Manche stellen irgendetwas auf dem Bildschirm dar oder spielen eine Melodie ab, andere simulieren ein kleines Programm. Eine echte Bedrohung für das System sind sie allerdings nicht – mit Sicherheit aber ziemlich lästig!

Tricks der Viren-programmierer (1)

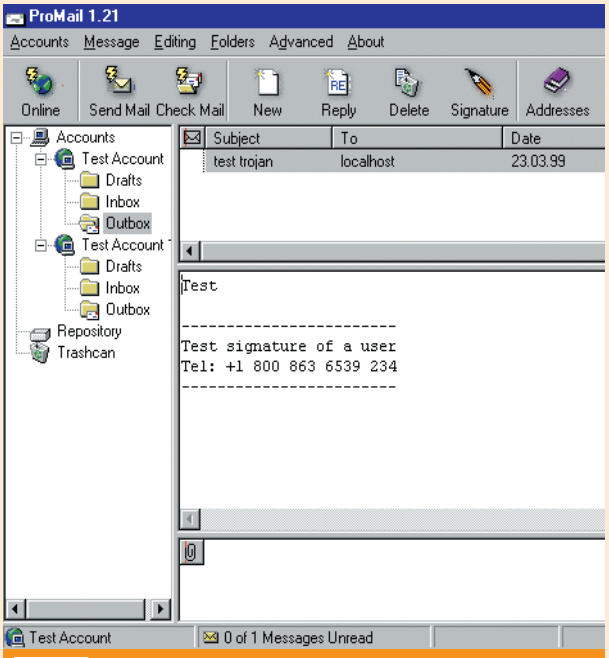
SCHWIERIGKEIT: FÜR FORTGESCHRITTENE

Viren bedienen sich verschiedenster Techniken, um zum einen möglichst gut vor Antiviren-Software geschützt zu sein und zum anderen ihre Schadensroutine ungehindert ausführen zu können. Einige besonders hartnäckige Viren-Typen wollen wir Ihnen an dieser Stelle kurz vorstellen. Beginnen wir zunächst mit den „speicherresidenten Viren“: Diese versuchen, die Kontrolle über das System an sich zu reißen, indem sie sich im Hauptspeicher des Rechners einnisten. So können sie unter anderem Festplattenzugriffe, Tastatureingaben, Druckausgaben und andere Funktionen überwachen und

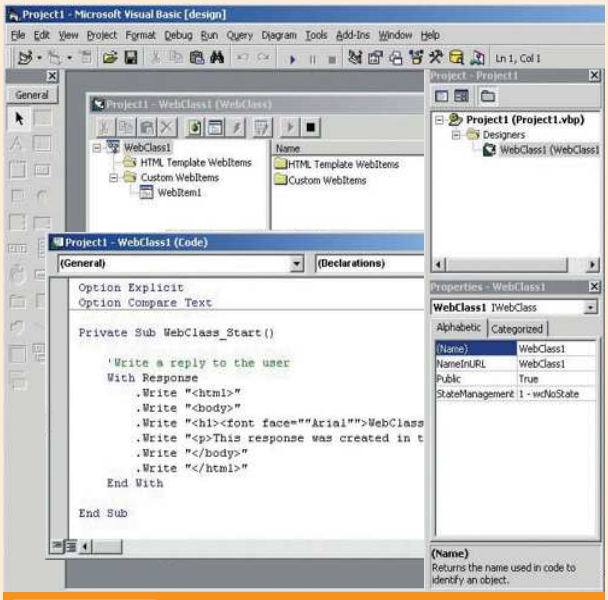


UNFREIWILLIGE HELFER Viren und Würmer verbreiten sich häufig über E-Mail-Clients wie das sehr verbreitete Outlook von Microsoft.

HAB DICH! Auf der Website www.trojaner-info.de finden Sie nicht nur eine Liste mit allen bekannten Trojanern, sondern auch Tools zur Bekämpfung.

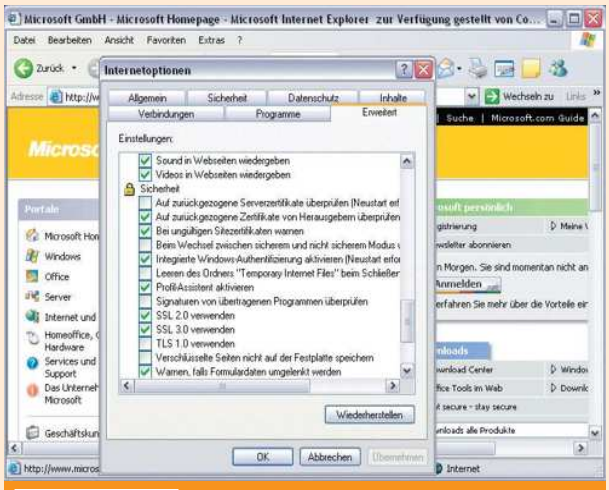


GETARNT Stealth-Viren tarnen sich, um Virenscanner zu täuschen. Der Trojaner „ProMail 1.21“ gibt sich zum Beispiel als E-Mail-Programm aus.



VB-SCRIPT-VIREN Die Programmiersprache Visual Basic ermöglicht es, auf fremde Rechner Code zu übertragen und ihn auch auszuführen.

SICHERHEITSRISIKO JAVA Mit der häufig im Internet benutzten Programmiersprache Java lässt sich der Rechner eines Surfers „fernsteuern".



SICHERHEITS-CHECK Wasserdichte Browser-Einstellungen sind sehr wichtig, um sich vor Gefahren, die von ActiveX, VB oder Java ausgehen, zu schützen.

manipulieren. Residente Viren bleiben nach ihrer Ausführung aktiv und können ihre Schadensroutine zu einem späteren Zeitpunkt ausführen. Ist der speicherresidente Virus erst einmal aktiv, kann er sofort andere Dateien infizieren. Nicht residente Viren werden übrigens erst beim Start des infizierten Programms aktiv. Sobald das Programm allerdings beendet wird, wird auch der Virus deaktiviert. Eine Variante der speicherresidenten Viren sind die so genannten Stealth-Viren – sie bedienen sich spezieller Tricks, um ihre Anwesenheit im System zu verschleiern. Dazu überwachen und manipulieren sie Zugriffe auf Programmdateien und das Inhaltsverzeichnis, um Virenscannern ein sauberes System vorzugaukeln. Soll beispielsweise die Größe einer infizierten Datei ermittelt werden, zieht der Stealth-Virus die Größe des Virus-Codes von der tatsächlichen Dateilänge ab und täuscht so eine korrekte Programmlänge vor. Doch Stealth-Viren sind sogar noch gerissener: Wird eine Programmdatei nicht ausgeführt, sondern nur gelesen (zum Beispiel von einem Virenscanner), entfernt der Virus aus der zu lesenden Datei den Viruscode, so dass die Antiviren-Software den Virus nicht in der Programmdatei finden kann.

Tricks der Virenprogrammierer (2)

SCHWIERIGKEIT: FÜR FORTGESCHRITTENE

Ein weiterer Trick, den sich die Virenprogrammierer von der Natur abgeschaut haben, ist die Fähigkeit zur Veränderung. Computerviren tun dies auf zwei verschiedene Arten. Die „verschlüsselten Viren" verstecken sich vor Virenscannern, indem sie ihren eigenen Programmcode transformieren. Der Virus konvertiert sich dabei selber in verschlüsselte, unleserliche Zeichen, die von Antivirenprogrammen nicht erkannt werden können. Doch verschlüsselte Viren können nicht auf ewig unerkannt bleiben – um sich zu verbreiten, muss sich der Virus wieder dekodieren und läuft somit Gefahr, entdeckt zu werden. Die nächste und gleichzeitig viel effektivere Form der Verwandlung findet man bei den „polymorphen Viren": Ihre Mutation besteht darin, dass sie ihren eigenen Programmcode manipulieren und so bei jeder Infektion anders „aussehen". Bestimmte Befehle Ihres Programmcodes werden dabei auf unterschiedliche Weise codiert. Um es Virenscannern noch schwerer zu machen, sind polymorphe Viren zudem noch verschlüsselt. Ein polymorpher Virus kann unter Umständen mehrere Milliarden verschiedener Mutationen erzeugen und so seine Erkennung nahezu unmöglich machen.

Bedrohungen aus dem World Wide Web

SCHWIERIGKEIT: FÜR FORTGESCHRITTENE

Einige Viren, die sich im Internet tummeln, machen bereits das bloße Surfen zu einem echten Sicherheitsrisiko. Besonders der weit verbreitete Internet Explorer von Microsoft ist daran nicht unschuldig. Viren könnten es sich theoretisch zunutze machen, über das Microsoft-spezifische ActiveX Programmcode von einem (Internet-)Server auf den Rechner zu übertragen und dort auszuführen. Trojanische Pferde nutzen diese Sicherheitslücke bereits seit geraumer Zeit. Funktionsfähige Viren dieses Typs sind laut H+BEDV Datentechnik (Hersteller des Virenscanners Antivir) aber noch nicht existent. Eine reale Gefahr bilden da schon „VB-Script-Viren" die auf Microsofts Programmiersprache Visual Basic (VB) aufsetzen. Das VB-Script kann dazu verwendet werden, Programmcode von einem Web-Server auf den heimischen Computer zu übertragen und auch auszuführen. Es genügt bereits das Ansehen einer Website mit dem Internet Explorer, um den eigenen PC zu infizieren. Um dieser Gefahr entgegenzuwirken, können im IE entsprechende Einstellungen vorgenommen werden. Auch die bei der Herstellung von Websites sehr häufig verwendete Sprache Java wird von Virenprogrammierern missbraucht. Java-Applets, die häufig in Browsern zur Animation oder Steuerung bestimmter Funktionen verwendet werden, können auch kritische Operationen ausführen wie unbemerkt etwas auf die Festplatte des Surfers schreiben. FRANK NEUPERT

Das MSI Quartett

für superschnell und supergünstig!

Mainboard KT4V-L

- VIA® KT400 mit 8x V-Link unterstützt AMD® Athlon™ XP 2600+/ Duron™ 1300 und höher
- 333 MHz FSB für AMD® Athlon™ XP
- DDR333 Speichertechnologie
- Thermal Protection
- 5.1 Channel Surround-Sound
- 6 PCI, **1AGP 8X**, 1CNR
- 6 USB 2.0 (MSI I/O:4+2)
- VIA® VT6103 LAN on-Board

Mainboard KT3V-L

- VIA® KT333 mit Unterstützung für AMD® Athlon™ XP 2800+/Duron 1300 und höher
- 333MHz FSB für AMD® Athlon™ XP
- DDR333 Speichertechnologie
- Thermal Protection
- 5.1 Channel Surround-Sound
- 6 PCI, **1AGP 4X**, 1 CNR
- 6 USB 2.0 (MSI I/O 4+2)
- VIA® VT6103 LAN on board

Mainboard K7N2-L

- Nvidia Crush18D mit Unterstützung für AMD® Athlon™ XP 2800+/Duron 1300 und höher
- 333MHz FSB für AMD® Athlon™ XP
- DDR400 Speichertechnologie (Dual Channel)
- Thermal Protection
- 5.1 Channel Surround-Sound
- 5 PCI, **1AGP 8X**, 1 ACR
- 6 USB 2.0 (MSI I/O 4+2)
- 10/100 LAN on board

Mainboard K7T266 Pro2-U

- VIA® KT266A mit Unterstützung für AMD® Athlon™ XP 2600+/Duron 1300 und höher
- 266MHz FSB für AMD® Athlon™ XP
- DDR266 Speichertechnologie
- 5.1 Channel Surround-Sound
- 6 PCI, **1AGP 4X**
- 6 USB 2.0

CeBIT
HANNOVER
12. - 19. 3. 2003
Halle 22, Stand B06

Alternate Computerversand GmbH www.alternate.de, **Atelco Computer Event GmbH** www.atelco.de
Vobis Microcomputer AG www.vobis.de, **PC Spezialist Franchise AG** www2.pcspezialist.de.

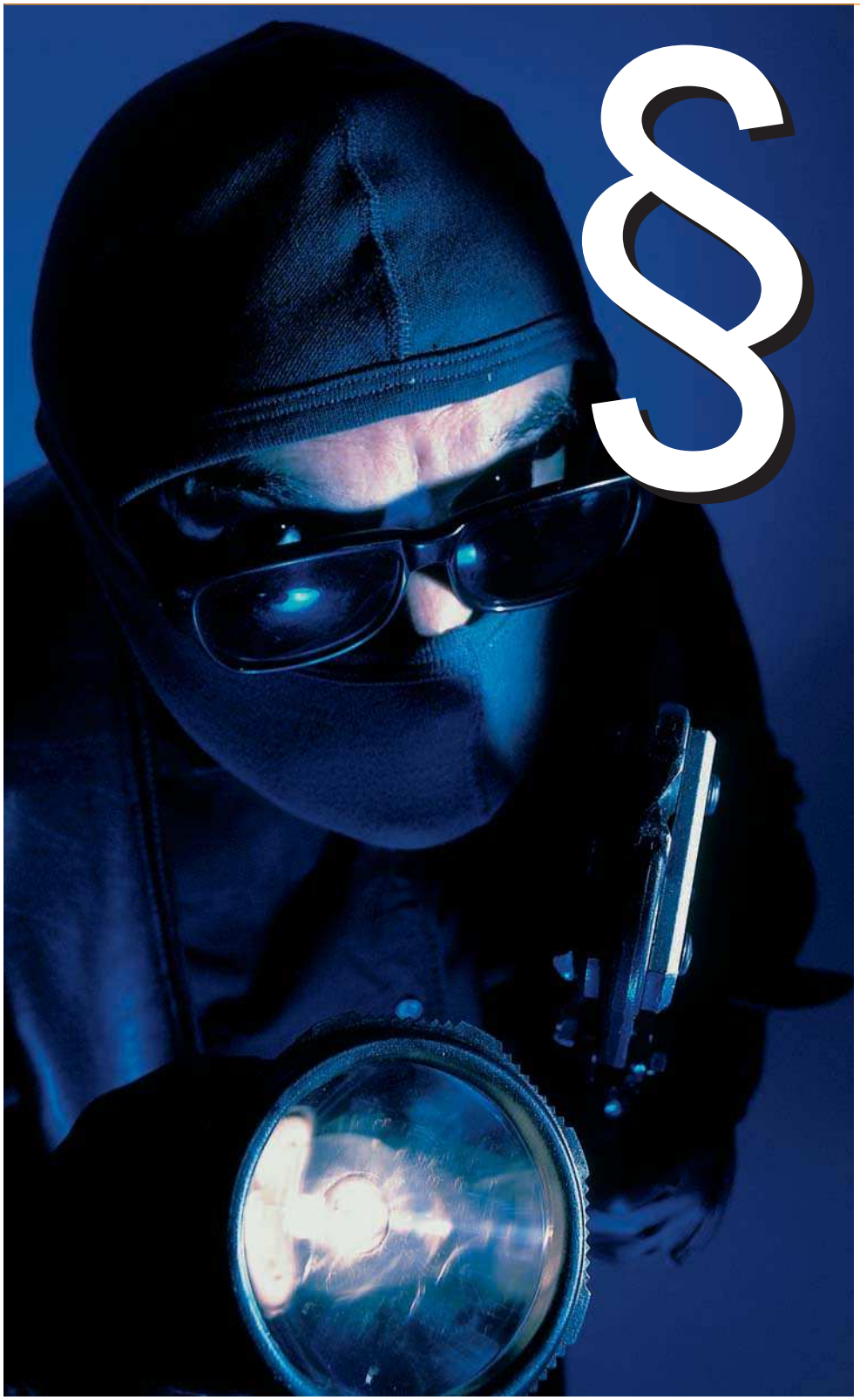
MSI™
MICRO-STAR INTERNATIONAL
Link to the Future

www.msi-computer.de

Weitere Bezugsquellen finden Sie auf der MSI-Website!
Treiber, Infos, Datenblätter–melden Sie sich im MSI PORTAL auf der Website von MSI an!
Alle eingetragenen Warenzeichen sind Eigentum der jeweiligen Firmen und Organisationen.
Änderungen und Irrtümer vorbehalten.

Cyber-Kriminalität

Hacker-Tricks enthüllt



Wer denkt, Hacker seien immer gewitzte Computergenies, irrt. „Hacker-Tools" und Sicherheitslücken erlauben es beinahe jedem, zum Hacker zu werden.

Wer Passwörter knackt, auf fremde Kosten surft und in Rechnersysteme einbricht, handelt nicht nur ungesetzlich, sondern sorgt auch dafür, dass die allgemeine Verunsicherung während eines Besuchs im Internet immer größer wird. Um sich wieder sicherer zu fühlen, ist es oftmals hilfreich, zu wissen, wie Hacker vorgehen – denn nur so lassen sich geeignete Schutzmaßnahmen treffen. Wir haben für Sie an dieser Stelle einige typische Hacker-Tricks zusammengestellt.

Angriffe auf Websites: DoS und Brute Force

SCHWIERIGKEIT: FÜR FORTGESCHRITTENE

Ein beliebtes Ziel vieler heutiger Hacker ist das Stören des Internetbetriebes großer Firmen. Durch gezieltes dauerhaftes Senden von Datenpaketen mit Antwortanforderung werden die Server dazu gebracht, die meiste Zeit diese Request-Anforderungen zu bearbeiten, was bei absichtlich abgebrochenen Datenpaketen dazu führt, dass die Server unter Umständen durch eine zu hohe Prozessverteilung regelrecht zusammenbrechen. Solche Angriffe sind gezielt und richten sich vor allem gegen große Firmenangebote, private Webseiten sind kaum in Gefahr.

Webseiten mit Zugangsportal, bei denen Passwort und Username abgefragt werden, sind ebenfalls immer wieder gerne Angriffsziel. Dabei werden so genannte Brute-Force-Tools eingesetzt. Als „Brute Force" wird

ein Algorithmus bezeichnet, der eine Buchstaben-/Zahlenkombination durch Ermittlung der einzelnen Zeichen aufdeckt. Brute-Force-Tools werden zum Beispiel gerne dort eingesetzt, wo sehr viele Benutzer durch Zugangsdaten in geschützte Bereiche gelangen können, zum Beispiel bei kostenpflichtigen Diensten oder bei großen Web-Hostern.

Brute-Force-Tools: Passwort-Knacker

SCHWIERIGKEIT: FÜR EINSTEIGER

Eine Brute-Force-Attacke geht so: Angenommen, der Hacker will in den durch Zugangsname und Passwort geschützten Bereich eines Anbieters für einen kostenlosen oder kostenpflichtigen Dienst. In dem Fall braucht er nur etwas Fantasie und ein Brute-Force-Tool. Die Fantasie ist nötig, um sich Usernamen zusammenzureimen, denn viele Nutzer melden sich unter ihrem realen Namen an. Die Wahrscheinlichkeit, einen hans.mueller@irgendwo.com zu finden, ist relativ groß. Diesen und weitere Usernamen trägt man in das Brute-Force-Tool ein. Als Nächstes wird durch Tests ermittelt, wie lang das Passwort sein muss – zum Beispiel acht Zeichen. Welche Zeichen genutzt werden dürfen, steht meist in der Rubrik „Hilfe“ im Zugangsbereich der Seiten. Im Brute-Force-Tool können dann genau diese Zeichen als Suchzeichen angegeben werden. Nehmen wir an, das gesuchte Passwort lautet „HANSMUEL“, dann arbeitet sich der Passwort-Knacker anhand der erlaubten Zeichen so vor: 1. Versuch: AAAAAAAA, 2. Versuch: BAAAAAAA und so weiter.

Das Brute-Force-Tool braucht dann nur die entsprechenden Kombinationen weiter auszuprobieren, bis es das komplette Passwort entschlüsselt hat.

Trace Routing: Der gläserne Internet-User (1)

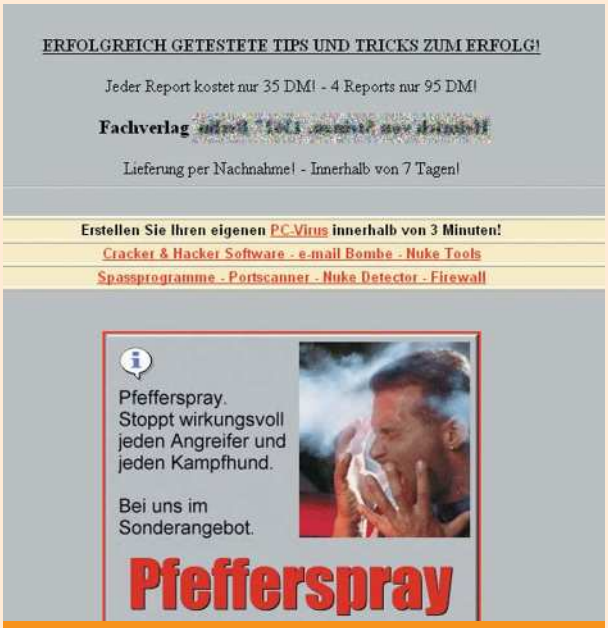
SCHWIERIGKEIT: FÜR EINSTEIGER

Eine sehr beliebte Methode, um Internetnutzer gezielt auf Adressdaten zu untersuchen, ist das „Trace Routing“. Trace-Programme dienen eigentlich dazu, die „Wegstrecke“ von Daten zurückzuverfolgen – zum Beispiel, um herauszufinden, warum das Erreichen einer bestimmten Webseite sehr lange dauert. Dazu nutzt man ein Trace-Programm. Dieses sendet an die eingegebene IP-Nummer Ping-Signale, dabei werden Datenpakete losgeschickt, deren Rückmeldung vom nächsten Server zeitlich gemessen werden, außerdem wird überprüft, ob die Pakete vollständig angekommen sind. Schaltet der erste Server den Weg zum nächsten (Ziel- oder Zwischenserver) frei, wird dieser Weg wieder gemessen und so weiter – so lange, bis das Ziel – der Rechner mit der gewünschten Internet-Adresse beziehungsweise IP-Adresse – erreicht wird. Und weil jeder Rechner im Internet eindeutig identifizierbar sein muss, lässt sich die komplette Adresse „tracen“. Über eine Whois-Abfrage bei der Internet-Domain-Vergabe erfährt man jetzt noch Adressdaten des Nutzers oder Betreibers – jedenfalls dann, wenn der Server nicht durch einen Provider abgeschottet wird. Zumindest jedoch kann man den Provider lokalisieren – und das überall auf der Welt (lesen Sie hierzu auch „Keine Chance für Hacker und Spammer“). Kleiner Tipp: Wenn Ihre Firewall meldet, dass Ihr Rechner „gescannt“ wurde, lässt dies darauf schließen, dass der Versender eines Trojanischen Pferdes wissen möchte, ob er Ihre Daten stehlen kann. Da die Firewall solche Versuche meist mit einer ermittelten IP-Nummer meldet, sollten Sie versuchen, diese zu ihrem Ausgangspunkt zurückzuverfolgen.

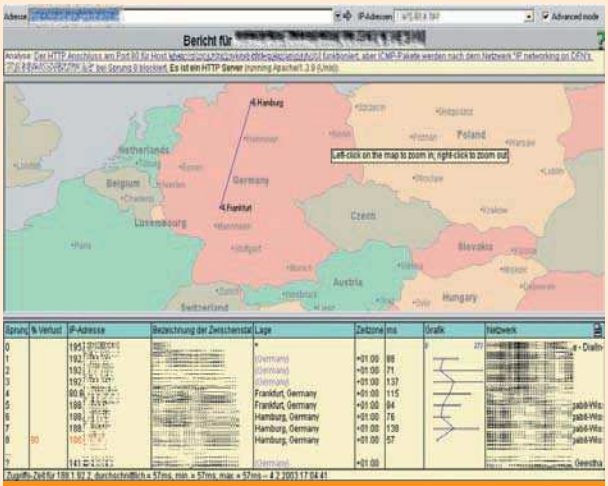
Portscans: Schon einen Trojaner eingefangen?

SCHWIERIGKEIT: FÜR EINSTEIGER

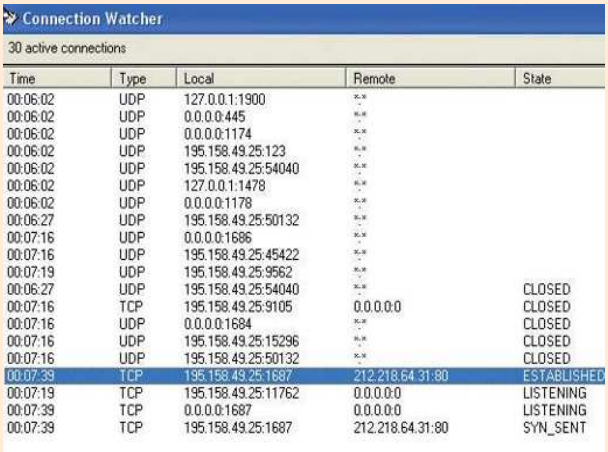
Trojanische Pferde (siehe auch Seite 18) haben folgende Eigenschaften: Sie teilen sich in einen Server- und einen Client-Teil auf. Der Client sitzt beim Versender des Trojaners, der Server nistet sich auf Ihrem PC ein. Er öffnet normalerweise nicht benötigte Ports, die als Schnittstellen für Datenübertragungen dienen. Ob ein PC von einem Trojaner infiziert ist, wird nun anhand eines „Portscans“ ermittelt: Man schickt vom Client



GEFAHRENQUELLE Auf solch fragwürdige Angebote, wie man selbst einen Virus „baut“, stößt man im Internet leider viel zu häufig.



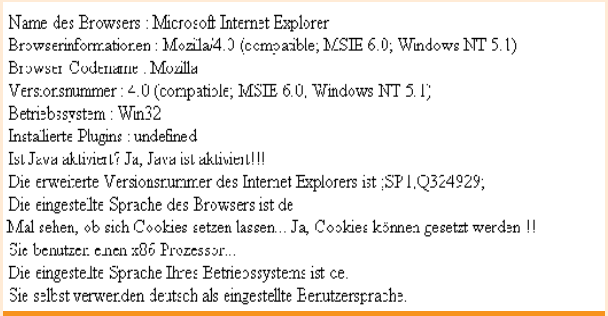
REISEROUTE Mit einem „Trace Router“ lässt sich anhand einer IP- oder Webadresse feststellen, von wo aus ein PC mit dem Internet verbunden ist.



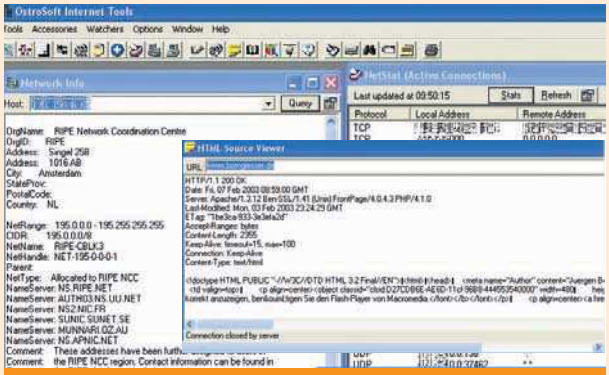
Time	Type	Local	Remote	State
00:06:02	UDP	127.0.0.1:1900	*:*	
00:06:02	UDP	0.0.0.0:445	*:*	
00:06:02	UDP	0.0.0.0:1174	*:*	
00:06:02	UDP	195.158.49.25:123	*:*	
00:06:02	UDP	195.158.49.25:54040	*:*	
00:06:02	UDP	127.0.0.1:1478	*:*	
00:06:02	UDP	0.0.0.0:1178	*:*	
00:06:27	UDP	195.158.49.25:50132	*:*	
00:07:16	UDP	0.0.0.0:1686	*:*	
00:07:16	UDP	195.158.49.25:45422	*:*	
00:07:19	UDP	195.158.49.25:9562	*:*	
00:06:27	UDP	195.158.49.25:54040	*:*	CLOSED
00:07:16	TCP	195.158.49.25:9105	0.0.0.0:0	CLOSED
00:07:16	UDP	0.0.0.0:1684	*:*	CLOSED
00:07:16	UDP	195.158.49.25:15296	*:*	CLOSED
00:07:16	UDP	195.158.49.25:50132	*:*	CLOSED
00:07:39	TCP	195.158.49.25:1687	212.218.64.31:80	ESTABLISHED
00:07:19	TCP	195.158.49.25:11762	0.0.0.0:0	LISTENING
00:07:39	TCP	0.0.0.0:1687	0.0.0.0:0	LISTENING
00:07:39	TCP	195.158.49.25:1687	212.218.64.31:80	SYN_SENT

AUFPASSER Ein „Connection Watcher“ überprüft die Ports eines PC auf ungewollten Datentransfer und zeigt an, welche Verbindungen aktiv sind.

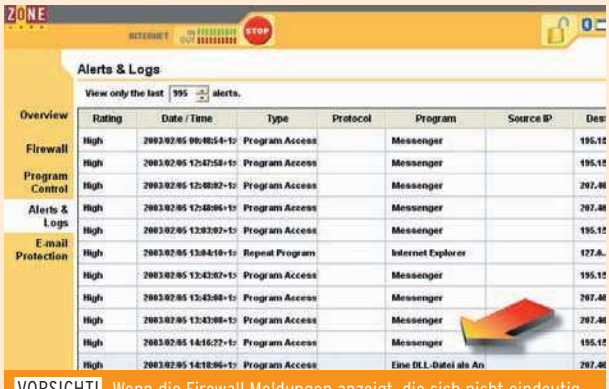
ABTASTUNG Ein Port-Scanner überprüft offene Ports eines im Internet angemeldeten PCs, dessen IP-Nummer bekannt ist.



BROWSER-TRANSPARENZ Diese Informationen lassen sich in Javascript durch einen einzigen Befehl und verschiedene Objekte rauskriegen.



TOOLSAMMLUNG Netzwerkadministratoren greifen oft auf kleine Tools zurück, mit deren Unterstützung sie Informationen über Surfer erlangen.



VORSICHT! Wenn die Firewall Meldungen anzeigt, die sich nicht eindeutig einem Programm zuweisen lassen, kann ein „Keylogger" aktiv sein.

aus eine Anforderung an die entsprechenden Portadressen, die vom Trojaner benutzt werden, und erfährt so, ob die Ports „geöffnet" oder „geschlossen" sind. Geöffnet bedeutet, dass der Server nun vom Client kontrolliert wird und Ihr PC ab sofort alle wichtigen Daten offen legt. Nun könnte man noch einen „Keylogger" benutzen. Der wird via Client-Server auf Ihrem PC abgelegt und protokolliert alle Ihre Tastatureingaben, sammelt diese in Datenpaketen und schickt sie an den unbekannten Empfänger. Haben Sie heute bei Ihrer Online-Bank schon Ihre PIN eingegeben? Und sind Sie sicher, dass die außer Ihnen niemand kennt? Vielleicht wäre der Einsatz einer Firewall doch sinnvoll, oder?

Das hat uns noch gefehlt: Script-Kiddies ...

SCHWIERIGKEIT: FÜR EINSTEIGER

Wenn Sie öfters im Internet aktiv sind, könnte es sein, dass Sie schon mal über den Begriff „Script-Kiddies" gestolpert sind. Gemeint sind damit eigentlich nur die vielen Nutzer diverser „Construction Kits" – das wiederum sind „Baukästen" zum Zusammensetzen von Viren, Trojanern, „Kill-Programmen" und dergleichen. Die Bauteile liegen meist in Form entsprechender Script-Sprachen wie Visual Basic vor und eignen sich dank der eingebauten Systemzugriffe sehr gut für böse Fallen. Und weil diese Construction Kits kinderleicht in der Bedienung sind, setzen sich des Öfteren Schüler oder pubertierende Teenies hin und basteln die einhundertste Abart des „Kurnikova"- oder des „LoveLetter-Virus". Das ist nicht originell, das ist nicht cool, das ist nur dämlich. Denn es ist schon vorgekommen, dass in entsprechenden Virusscripts neben fehlerhaftem Code auch noch die E-Mail-Adresse des Urhebers versteckt war. Dummerweise schaffen es etliche „Kiddies" aber auch immer wieder, einen funktionierenden Script-Virus in Umlauf zu bringen. Mit „Hacken" hat das überhaupt nichts zu tun, hier geht es nur ums Angeben – leider mit sehr negativen Folgen, wie die Antivirenprogramm-Hersteller immer wieder feststellen müssen.

Keylogging – „Ich sehe das, was du tippst!"

SCHWIERIGKEIT: FÜR EINSTEIGER

Eine große Gefahr beim Download von Tools aus dem Internet besteht in der unabsichtlichen und unbemerkten Installation eines Keyloggers. Diese kleinen, von Hackern gern genutzten Programme arbeiten komplett im Hintergrund, es gibt keine direkten sichtbaren Hinweise auf Aktivitäten – jedenfalls nicht so, wie man es von Windows-Programmen gewöhnt ist. Stattdessen arbeiten Sie ganz normal weiter, Sie tippen Briefe und Dokumente, Sie geben Ihre Passwörter ein, Sie chatten oder schreiben E-Mails. Und der kleine Keylogger sammelt Zeichen für Zeichen alles, was Sie über die Tastatur eingeben. Sind mehr als 1.000 Zeichen zusammen, „baut" er eine Datei und schickt diese beim nächsten Mal, wenn der Nutzer eine Internetverbindung aufbaut, an einen unbekannten Empfänger. Da jeder Internetzugang erst einmal Abgleichdaten vom und zum Provider übermittelt, fallen die paar Byte überhaupt nicht auf.

Keylogger erkennt man nur an ihren charakteristischen Prozessen oder durch spezielle Suchprogramme. Um einen Keylogger aufzuspüren, müssen Sie den Taskmanager unter Windows aufrufen (einfachste Methode ist „ALT" + „Ctrl" + „ENTF") und dort die Registerkarte „Prozesse" aktivieren. Ist der Keylogger halbherzig programmiert, läuft er erkennbar als Nutzerprogramm, hartnäckigere Versionen werden allerdings als Systemprogramme getarnt. Hier müssen Sie dann herausfinden, ob ein Prozess besonders aktiv ist, sobald Sie zum Beispiel Texte eingeben. Der einzige wirkliche Tipp, der gegen Keylogger hilft, lautet aber: Laden Sie keine Programme von Seiten, die Ihnen nicht vertrauenswürdig erscheinen.

Der gläserne User (2): Zeigen Sie Profil

SCHWIERIGKEIT: FÜR EINSTEIGER

Die bisher vorgestellten Aktivitäten sind schon sehr speziell und benötigen etliches an Fachwissen und Hacker-Vorbildung

„Barney" (Ex-Hacker)

Werdegang:
Vormals Hacker aus Passion, hat Hobby zum Beruf gemacht.

Derzeitige Tätigkeit:
Sucht Sicherheitslücken in Webservern und Online-Systemen, entwickelt Sicherheitssysteme.

Hacker-Interview

„Barney" war Hacker aus Passion. Er hat selbst Trojanische Pferde mitentwickelt, die immer noch im Internet kursieren. Sein Hobby hat er jetzt zum Beruf gemacht.

Was hat dich daran gereizt, die PCs anderer Internet-User auszuspionieren?
Vor allem die Unbedarftheit, mit der viele Internet-User ins Netz gehen. Und hier vor allem die der Microsoft-User. MS hat mit dem Internet Explorer von Anfang an bewiesen, dass man Sicherheitsaspekte außer Acht lassen kann, wo man nur will. Outlook Express ist ein gutes Beispiel für lückenhafte Internet-Software, zu sehen auch an den vielen Script-(Makro-)Viren. Man braucht einen gut getarnten Trojaner nur als das ultimative Tool in Download-Pools anzupreisen, schon lädt sich jeder das Ding auf den Rechner, installiert es – und sitzt in der Falle. Allein diese Vorstellung reicht aus, um mit solchen Geschichten weiterzumachen.

Welchen anderen Hacker-Aktivitäten gehst du jetzt noch nach?
(Lacht): Na ja, im Grunde versuche ich natürlich alles, um Schwachstellen, jetzt vor allem auf Webservern, aufzudecken. Dazu gehören unter anderem Portscans, dazu gehören Brute-Force-Attacken, aber auch Eingriffe in die Programmstrukturen der Server-Applikationen. Natürlich nur, um den Betroffenen zu zeigen, wo Sicherheitsmängel sind und wie sie abzustellen sind.

Was machst du mit den Daten, die du „findest"?
Grundsätzlich ist es so, dass ich den Betroffenen sage, was ich „gefunden" habe, dass ich ihnen zeige, wo zum Beispiel Passwörter abgelegt werden, bevor sie „geschützt" sind, und Tipps zum Ablegen von Dateien gebe. Viele sind erstaunt, persönliche Daten plötzlich auf einer Diskette oder CD von mir wiederzufinden, sie begreifen nicht, dass sich zwischen Eingabe und Ausführung immer noch Zwischenschritte vom System befinden, über die sich Datenspione – gleich welcher Art – einklinken können.

Wie würdest du die Sicherheitsmaßnahmen bei Privat-Usern, Firmen und Institutionen heutzutage einschätzen?
Bei den Firmen und Behörden hat sich das Bewusstsein für das Sicherheitsproblem stark erweitert. Das größte Problem einer Firma sind aber immer noch die Mitarbeiter. Sie installieren oft auf dem Firmenrechner Programme, die sie von zu Hause mitbringen, ohne daran zu denken, dass hier bereits eine Sicherheitslücke entstehen kann. Das Sicherheitsbewusstsein bei Privat-Nutzern liegt völlig daneben. Es wird eher darauf verzichtet, mit der Kreditkarte im Internet einzukaufen, als die eigenen Mails mit Verschlüsselungsprogrammen zu schützen.

Welche Maßnahmen empfiehlst du, um Hackern das Leben schwer zu machen?
Grundsätzlich nie darauf vertrauen, dass Virenchecker oder Firewall-Programme alles für einen regeln. Die standardmäßigen Firewall- und Antivirenprogramme sind kein Garant für vollen Schutz. Außerdem sollte man nie Programme laden und installieren, die nicht irgendwo schon mal getestet wurden. Passwörter und Usernamen gehören niemals auf die Festplatte – und schon gar keine Informationen über Zahlsysteme wie Kreditkarten. Spurenlöscher und Kryptographie-/Steganographieprogramme sind weitere sinnvolle Hilfen.

– auch wenn sie relativ schnell einsetzbar sind, sofern man die richtigen Tools zur Hand hat. Es geht aber auch einfacher, obwohl diese Methode mit dem eigentlichen „Hacken" nur noch die Grundlagen gemein hat. Viele Website-Betreiber benutzen auf ihren Homepages Mechanismen, die einen normalen Websurfer ziemlich transparent erscheinen lassen. Dazu gehören oft nur wenige Zeilen Code einer Scriptsprache, die einfach in die HTML-Struktur einer Seite eingebunden werden. Javascript zum Beispiel enthält zwar im Gegensatz zu VB-Script oder ActiveX keine Möglichkeit, direkt auf Dateien zuzugreifen, aber es arbeitet mit besonderen Befehlen zur Beeinflussung von Webelementen. Dazu gehört zum Beispiel das Abfragen von Browser-Systemvariablen wie Version oder Betriebssystem.

Ihr Browser verrät Sie: Webmaster spionieren

SCHWIERIGKEIT: FÜR EINSTEIGER

Heute muss keiner mehr tagelang auf der Tastatur „herumhacken", um Zugangspasswörter auszuspionieren. Ein paar Zeilen Code einer Programmiersprache reichen aus, um die ganze Angelegenheit zu automatisieren. Sogar das unscheinbare Javascript kitzelt Ihrem Browser mehr Informationen heraus, als Ihnen lieb sein kann. Neben den Grundinformationen wie Browsername, Version und so weiter kann ein Webmaster bestimmte Abfragen einbinden, um festzustellen, ob ein Java-Applet zusätzlich gestartet werden kann. Sollte die Abfrage ergeben, dass Java im Browser aktiv ist, hat ein Hacker die Möglichkeit, ein Java-Applet auszuführen. Was zunächst kompliziert klingt, ist im Grunde recht einfach:

Sobald das Script vom Browser erfährt, dass Java implementiert ist und Java-Applets automatisch gestartet werden können, aktiviert es ein in die Website eingebautes Applet, das wiederum eine DOS- oder Windows-Datei auf den Rechner des Besuchers der Seite schickt, sofern dieser nicht gegen solche „Übernahmen" geschützt ist. So könnte man unter bestimmten Umständen auch einen Keylogger einschleusen. Oder ein VB-Script, das mit Ihrem Rechner allerhand Unfug anstellen kann. Der Netscape-Browser kann sogar dazu gebracht werden, die IP-Nummer und den Namen des Hostrechners freizugeben. Mit solchen Informationen kann ein geübter Web-Hacker schon einiges anfangen. Und wenn Sie sich als Internet-Explorer-Benutzer wundern, warum Sie nicht auf bestimmte Webseiten gelangen und stattdessen kurz darauf wieder bei der zuletzt besuchten Seite sind: Der Webmaster fragt nach dem Namen des Browsers. Findet er ein „Internet Explorer", fragt er kurzerhand über ein Script die History der zuletzt besuchten Webseiten ab und schickt Sie dorthin zurück. Also: Im Internet ist niemand anonym. Schon gar nicht ohne Schutzsysteme. Und nur die schützen halbwegs vor Hackern und Crackern. FRANK NEUPERT/ JÜRGEN BORNGIESSER

Trojaner und Backdoor-Systeme

Gefahr durch Hintertür

Backdoor-Systeme und Trojanische Pferde sind kleine Programme, die unbemerkt Daten, Passwörter und sogar Tastatureingaben an einen Empfänger irgendwo im Internet übermitteln.

Es passiert schnell und meist unbemerkt: Man installiert ein kleines, meist kostenloses Programm aus dem Internet, doch anstelle der neuen Funktionen erscheint nur ein „Datei xxx nicht gefunden". Das vermeintlich defekte Programm wird deinstalliert oder gelöscht. Schon kurze Zeit später ist dieser Vorgang aber vergessen, jedenfalls so lange, bis die nächste Telefonrechnung kommt. Nein, hier war kein Dialer am Werk, der Einzelverbindungsnachweis zeigt nur eine immens hohe Anzahl von Gebühreneinheiten bei der Provider-Einwahl. Des Rätsels Lösung: Das „defekte" Programm war ein so genanntes Trojanisches Pferd. Und der „Insasse" nutzt kostenlos Ihren Internetzugang für seine Zwecke. Der „Insasse" – das ist nämlich der Programmierer des Trojanischen Pferdes, der ab sofort Ihren Computer kontrolliert.

Mit dem Begriff „Trojanisches Pferd" (oder auch oft nur „Trojaner" genannt) werden allgemein Programme benannt, die schädlichen (nicht schadhaften!) Code enthalten. Ein Trojanisches Pferd ist als solches eigentlich nicht erkennbar. Es verbirgt sich oft hinter scheinbar nützlichen Programmen aus dem Internet, bietet Funktionen, die das Opfer sogar gut gebrauchen kann, und arbeitet ohne Ihr Wissen still und leise im Hintergrund.

Back Orifice – System mit Hintertürchen

SCHWIERIGKEIT: FÜR FORTGESCHRITTENE

Als in diversen Download-Pools das erste Mal ein Programm namens „Back Orifice" als Steuerprogramm für Systemadministratoren auftauchte, waren diese von der Fülle an neuen Funktionen zur Überwachung von Netzwerk-Servern recht angetan. Dabei hätte man schon beim Namen der Programmierer stutzig werden müssen: Der Name

WAS IST?

Backdoor-Tool
Verfügt unsichtbare Funktionen, die eine Kommunikation mit weiteren Benutzern ermöglichen.

Kryptographie
Spezielle Algorithmen zur Verschlüsselung sensibler, geheimer Daten mit Codeschlüsseln

Prozess
Jedes System- und Anwendungsprogramm, das im Vorder- oder Hintergrund läuft

PIN/TAN
Persönliche Identifikations-Nummer und Transaktions-Nummer für Online-Banking

„Cult of the Dead Cow“ wies zwar nicht eindeutig, aber zumindest halbwegs darauf hin, dass dieses Programm nicht ganz so harmlos war, wie es schien. Tatsächlich gab es eine „Hintertür“ in Back Orifice, genauer gesagt ein Scheunentor, das über die Netzwerk-Kommunikation und die Datenports des PCs mittels eines Server-Programms Verbindung zur „Heimat“ der Hacker aufnahm und Daten an die dortigen Adressen verschickte. Auf diese Weise konnte der Netzwerkrechner tatsächlich von außen abgefragt und regelrecht ferngesteuert werden.

Trojaner sind meist rund um die Uhr aktiv. Das eigentliche Trojanische Pferd installiert sich so in ein System, dass es jederzeit mit dem Start des PCs ebenfalls gestartet wird. Unter den älteren Windows-Versionen ging dies über „SYSTEM.INI“ und „WIN.INI“, wobei ein „Load“- oder „Run“-Befehl das eigentliche Backdoor-Programm zur Ausführung brachte. Bei den neueren Windows-Versionen ist es noch problematischer, das Trojanische Pferd aufzuspüren. Hier wird eine Startinformation in die Registry-Datenbank eingetragen, die beim Hochfahren des Systems den Trojaner aktiviert. Zudem gibt es auch Trojanische Pferde, die erst gestartet werden, wenn sich ein Tarnprogramm aktiviert hat. Das kann zum Beispiel ein Tool wie das Remote-System sein, aber auch ein E-Mail-Client, den man täglich mehrmals einsetzt.

Das können Trojanische Pferde anrichten

SCHWIERIGKEIT: FÜR EINSTEIGER

Im Vordergrund der Aktivitäten stehen das Ausspionieren von Passwörtern und personenbezogenen Daten sowie das „Öffnen“ von nicht gesicherten Port-Adressen. Es gibt Trojanische Pferde, die jeden Tastaturklick aufzeichnen und so alle Eingaben an ein Empfängersystem übermitteln. Dazu klinkt sich der Trojaner in die Tastaturabfrage ein und legt alle entnommenen Tastencodes in einer fortlaufenden Datei an. Bei Erreichen einer bestimmten Menge an Daten wird dieser Datenstrom über den offenen Port an den Hacker geschickt. Wehe dem, der Geheimdaten wie PIN- und TAN-Nummern von Online-Konten eingibt.

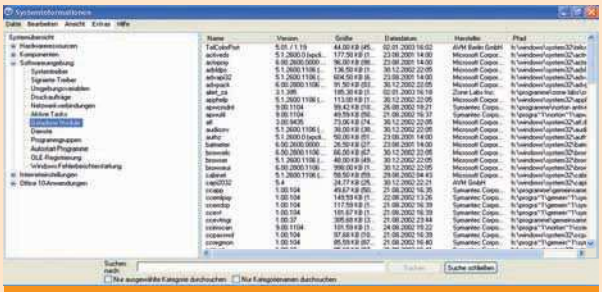
Andere Trojanische Pferde überprüfen die Online-Verbindung zum Provider und versuchen, die Passwortabfrage abzufangen. Sind die Zugangsdaten übermittelt, kann der Versender des Trojanischen Pferdes mit Ihren Zugangsdaten jeden Blödsinn anstellen: kostenpflichtige Webseiten besuchen und sich dort anmelden, E-Mails unter Ihrem Namen schreiben und Ähnliches. Dabei sind etliche Trojaner so gut programmiert, dass Filter in der Lage sind, wichtige von unwichtigen Daten zu trennen und nur die relevanten Informationen zu verschicken.

Eine weitere Gruppe Trojanischer Pferde versteckt ein Server-System auf dem PC, übernimmt einen der Ports für den Zugriff eines Kontrollsystems und ermöglicht so die totale Kontrolle über alles, was auf dem Rechner gespeichert ist. Das entsprechende Client-Programm des Trojaners ist ein „Port-Scanner“: Er überprüft Rechner im Internet auf durch den Server des Trojaners geöffnete Ports und kann so einem Hacker übermitteln, ob der Rechner von außen Zugriff erlaubt. Theoretisch könnte auf diese Weise sogar ein komplettes System zum Absturz gebracht werden. In der Praxis sind solche als „Nuke“-Programme bekannten Tools aber eher zu Demonstrationszwecken zu finden. Der eigentliche Nutzen für den Hacker: Er will Daten sammeln und keine Dateien zerstören.

Trojanische Pferde suchen und finden

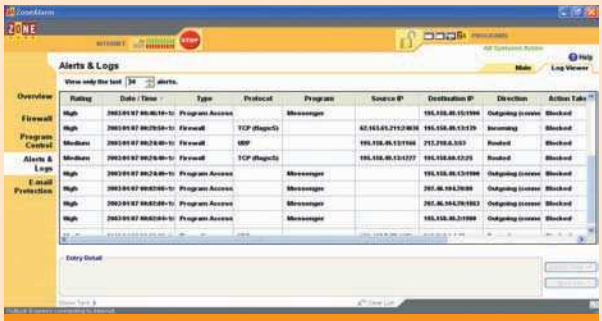
SCHWIERIGKEIT: FÜR FORTGESCHRITTENE

Die allererste und sinnvollste Maßnahme ist das Installieren eines guten Virenscanners mit sofortigem Update der Virendefinitionsdateien. Die meisten professionellen Virenscanner erkennen inzwischen auch Trojanische Pferde. Allerdings – und das ist der Haken – tauchen immer wieder modifizierte Versio-

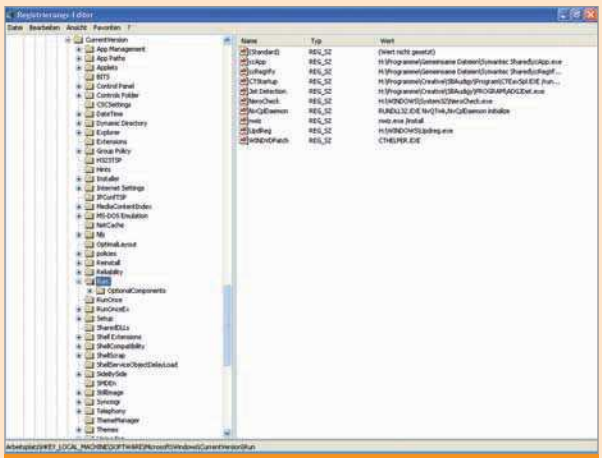


PROGRAMM-AKTIVITÄTEN Unter „Softwareumgebung/Geladene Module“ bekommen Sie einen Überblick über die aktiven Programmdateien.

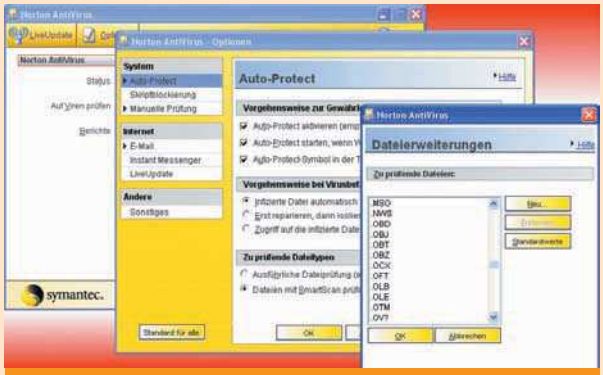
TROJANER-INFO Die Seiten unter www.trojaner-info.de informieren über aktuelle Trojaner-Aktivitäten und geben praktische Tipps.



VERBINDUNGEN Offene Kommunikations-Ports lassen sich mithilfe einer richtig konfigurierten Firewall schnell ausfindig machen.



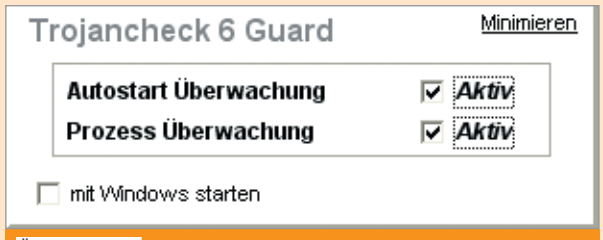
VERSTECKT Trojaner-Aktivitäten sind ohne Hilfsmittel kaum feststellbar. Es gibt in der Registry eventuell Einträge, die auf Trojaner hinweisen.



ANTIVIREN-OFFENSIVE Viele Virenscanner können auch Trojaner aufspüren. Dazu muss der Scan allerdings auf alle Dateien ausgeweitet werden.

SCHUTZSCHILD Tools wie „Trojancheck" können Trojaner besser entdecken, da sie nicht nur Dateien, sondern auch Registry-Einträge überprüfen.

PROZESSKONTROLLE Unbemerkt im Hintergrund ablaufende Prozesse unter Windows sind normal. Trotzdem sollte man sie ab und zu prüfen.



ÜBERWACHUNG „Trojancheck" überwacht die Registry- und Prozesseinträge und meldet ungewöhnliche Vorgänge sofort.

nen der Ursprungs-Trojaner auf, die es den Virenscannern erschweren, diese nach signifikanten Inhalten der Dateien zu untersuchen. Außerdem sind neue Trojaner keine Seltenheit, die in ganz „normalen" Applikationen versteckt sind – da dürfte jeder Virenscanner Probleme mit der Erkennung bekommen. Eine weitere Schutzmaßnahme ist die Installation einer Firewall wie „ZoneAlarm" (siehe Artikel in diesem Heft). Nur sie ist in der Lage, unerlaubte Port-Aktivitäten aufzuspüren und anzuzeigen. Da ein Trojanisches Pferd nicht zwingend wie ein Virus wirkt und auch nicht die entsprechende Form hat, ist die Erkennung über Firewall-Systeme wahrscheinlicher – vor allem, wenn ein Server-Teil installiert und nicht genutzte Ports geöffnet werden. Um dies herauszufinden, muss die Firewall aber richtig konfiguriert sein, um erlaubte und nicht erlaubte Zugriffe einwandfrei erkennen zu können.

Spezielle Anti-Trojaner-Tools sind eine weitere gute Maßnahme für das Aufspüren von Trojaner-Aktivitäten. Ein sehr bekanntes und gutes Programm ist „Trojancheck" (www.detektei-ses.de). Es verfügt über Routinen, die ein Aufspüren selbst unbekannter Trojaner ermöglichen, da es die Kommunikation von Applikationen mit dem System anhand von Programmroutinen erkennen kann. Zwar bietet auch „Trojancheck" keinen hundertprozentigen Schutz gegen den Befall mit Trojanischen Pferden, doch zusammen mit den beiden anderen Maßnahmen ist die Gefahr um etliches verringert.

Tipps zum Auffinden von Trojanern

SCHWIERIGKEIT: FÜR FORTGESCHRITTENE

Stellen Sie das Antiviren-Programm so ein, dass nicht nur EXE-, COM- und DLL-Dateien, sondern wirklich alle Dateien auf dem PC untersucht werden. Das kostet zwar mehr Zeit, bietet aber auch wesentlich mehr Sicherheit. Vorsicht beim automatischen Entfernen gefundener Trojaner-Dateien – unter Umständen wird das System instabil. Versuchen Sie zuerst das entsprechende Trägerprogramm zu deinstallieren. Achten Sie bei Firewalls darauf, welche Ports aktiviert werden – und durch welche Programme. Wenn ein gerade neu installiertes Programm versucht, außerhalb der normalen Aktivitäten mit dem Internet zu kommunizieren, ist Vorsicht geboten. In den meisten Fällen handelt es sich um so genannte „Spyware" (siehe Artikel in diesem Heft), es kann aber auch ein Trojanisches Pferd sein.

Selbst für fortgeschrittene Benutzer ist das manuelle Aufspüren eines Trojanischen Pferdes sehr schwer. Viele Trojaner sind nur anhand von Einträgen in der Registry identifizierbar – und selbst das ist nur mit speziellen Trojaner-Suchprogrammen machbar. Kontrollieren Sie trotzdem die laufenden Prozesse auf dem Windows-Rechner (Taskmanager/Prozesse) und schauen Sie nach, welche Programm-Module Windows aktiviert hat. Dazu wählen Sie im Startmenü – Ordner „Zubehör/Systemprogramme" – den Eintrag „Systeminformationen". In „Softwareumgebung/Geladene Module" sehen Sie eine Übersicht über die gerade aktiven Programme sowie Informationen zum Hersteller. Finden Sie Einträge, die Ihnen unbekannt erscheinen, notieren Sie die Daten und versuchen Sie anhand dieser Informationen, genau diese Einträge untersuchen zu lassen.

Über das Systemprogramm „regedit" (zu finden im Windows-Ordner) können Sie die Registry von Windows einsehen. Trojaner nutzen meistens Auto-Run-Funktionen, um beim Hochfahren des Rechners aktiv zu werden. Die entsprechenden Einträge finden Sie hier: HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run\ sowie unter KEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnce\. Löschen Sie jedoch keinesfalls die Einträge, ansonsten kann das komplette Windows-System instabil werden. Versuchen Sie auch hier, die Informationen in den jeweiligen Analyseprogrammen auszuwerten. JÜRGEN BORNGIESSER

Sicher?

Sicher!

Sicher ist sicher – der neue ELSA LAN DSL-Router 4P kommt mit einer umfangreichen Sicherheitsausstattung einschließlich leistungsstarken Firewall-Funktionen und Anti-Viren-Schutz durch die Titanium-Edition der Anti-Virus Software von Panda. Dieser Router mit integriertem 4-Port-Switch ist ideal für die Anbindung von LANs und auch Clans ans Internet bzw. Multi-Player-Server. Jetzt im Fachhandel erhältlich. UVP: 99,00 Euro.

www.elsa.de

CeBIT
HANNOVER
12. – 19. 3. 2003
Halle 16, Stand D 06

ELSA

Sicher vor Spy- und Adware

Vorsicht, Spion an Bord!

Spyware oder Adware – das sind Bezeichnungen für eine besonders perfide Art der Spionage. Unbemerkt und geheim im Hintergrund melden kleine Computerprogramme jede Ihrer Aktivitäten im Netz.

Stellen Sie sich vor, Sie besuchen im Internet einen Webshop, einen Online-Kurs für JavaScript und die Website eines Computerspiel-Vertriebes. Und am nächsten Tag erhalten Sie plötzlich Angebote über Bücher, Software, DVDs sowie aktuelle Angebote zu Krediten, die Sie voraussichtlich nie nutzen würden. Zufall? Nein, eher das Ergebnis eines Downloads – denn viele kostenlose Programme haben ein Spionage-Programm an Bord, das unablässig sämtliche Netzaktivitäten an seinen Hersteller meldet. Diese Spionage hat nur ein Ziel: Man will Sie und jeden anderen Web-Surfer zum gläsernen Kunden machen. Das Kaufverhalten im Internet ist interessant für alle Firmen, die Produkte in Webshops anbieten, genauer gesagt für die Leute, die Ihr Verhalten im Internet auswerten, um Sie auf spezielle Angebote zu lenken. Das hört sich wiederum eigentlich ganz nett an – doch das so genannte User-Tracking nutzt schon lange Daten, die aus mehr als nur E-Mail-Adresse und Website-Verlauf bestehen.

Verräter: Cookies, Web-Bugs, Spion-Banner

SCHWIERIGKEIT: FÜR EINSTEIGER

Die einfachste Art, einen Internet-Surfer wiederzuerkennen, ist das Speichern einer kleinen Datei im temporären Speicher des Browsers. Dieses „Cookie“ enthält Codes über die besuchte Website, die Anzahl der Klicks sowie Informationen über die Verweildauer und den Inhalt des Einkaufskorbes, sofern dieser mit Waren belegt wurde. Cookies sind entgegen weitläufiger Meinung weder schädlich noch verbreiten sie direkt Informationen über den User, sie können jedoch vom Server aus gelesen und ausgewertet werden. Web-Bugs sind dagegen kleine Bildchen, meist nicht größer als 1x1 Pixel, ohne Alternate-Beschriftung (wird als Text anstelle des Bildes eingeblendet) und transparent (Formate: GIF, PNG). Sie sind faktisch unsichtbar und werden ebenfalls im temporären Speicher abgelegt, verweisen aber auf einen anderen Server-Standort als herkömmliche Bilddateien. Server, die solche Web-Bugs („Bug“ steht hier nicht für „Fehler“, sondern tatsächlich für „Käfer“) im temporären Speicher installieren, können durch die direkte URL-Verbindung Spion-Programme auf den lokalen Rechner übertragen. Werbebanner schließlich, die beim Anklicken auf bestimmte Angebote verweisen, können über Scripte kleine ausführbare Webprogramme aufrufen, die ebenfalls im temporären Ordner gespeicherte Informationen übermitteln. Eigentlich besitzen alle drei Spion-Systeme geringes Gefahrenpotenzial, zumindest was zerstörerische Kräfte angeht. Allerdings werden durch gesammelte Informationen im temporären Speicher viele User-Details freigegeben, die über Server-Aktivitäten

WAS IST?

Cookies
Ungefährliche Datei, die Informationen über das Surfverhalten eines Benutzers speichert.

Web-Bugs
Hierdurch werden über direkte URL-Verbindungen Spion-Programme auf Ihren PC geschleust.

Adware
Programme, die an Bord von Shareware-Tools Werbung einblenden und spionieren.

Ad-Aware
Tools die Ihren Rechner nach Spyware scannen und gefundene Spione unschädlich machen.

nach „außen“ gelangen, was durch alle drei Spion-Arten geschieht. Diese drei Datei-Arten wirken wie Markierungen oder Positionslampen im Internet. Wenn Sie diesen Spionage-Systemen keine Chance geben möchten, empfiehlt es sich, nach jedem Web-Besuch den temporären Speicher zu löschen. Bedenken Sie aber bitte, dass dabei auch Warenkorb-Cookies verloren gehen.

Adware – Spionieren und spionieren lassen

SCHWIERIGKEIT: FÜR EINSTEIGER

In vielen Download-Pools werden werbefinanzierte Shareware-Versionen von Programmen angeboten. Diese blenden dauerhaft Werbebanner während des Programmaufrufes ein. Bekannt für diese Werbung sind vor allem zwei Firmen aus den USA, wo diese Art des User-Tracking gang und gäbe ist: „Radiate/Aureate“ und „Gator“. In vielen bekannten Shareware-Programmen, zum Beispiel Download-Managern wie „Getright“, ist ein entsprechendes Programm-Modul enthalten, das bei der Installation des Hauptprogramms ebenfalls auf der Festplatte eingerichtet wird. Diese Spion-Programme sind manchmal sogar so dreist, eine eigene Registrierung zu verlangen. Dabei werden Name und Anschrift, Telefon, Internetadressen und persönliche Vorlieben verlangt. Sobald die Informationen eingetragen sind, verschafft sich die Software meist noch folgende Infos: Betriebssystem und Rechnerdaten, Registrierungsdaten, Einträge in der Registry, E-Mail-Accounts, installierte Vollversionen.

Diese Daten werden über offene Ports der Internetverbindung an den Hersteller der Spion-Systeme verschickt. Und dann bekommen Sie Werbemails (Spam), bis das E-Mail-Postfach überquillt, denn diese Daten gehen auch an andere Firmen über. Unverschämt: Die Spion-Programme übermitteln weitaus mehr Daten, als sie dürften, sie kontrollieren Neuinstallationen und lassen sich selbst bei Deinstallation des Trägerprogramms nicht mehr entfernen. Die Übermittlung der Daten geschieht ohne Bestätigung durch und Hinweis an den Benutzer. Selbst wenn die Shareware-Version durch Registrierung zu einer Vollversion umgewandelt wird, bleibt die Adware aktiv. Um sich dagegen zu wehren, ist der Einsatz eines Spion-Blockers wie Ad-Aware zwingend notwendig. Nur so können einzelne DLLs (Dynamic Link Libraries – Programmbibliotheken) entfernt werden, die selbstständig weiterarbeiten, auch wenn das Hauptprogramm entfernt wurde.

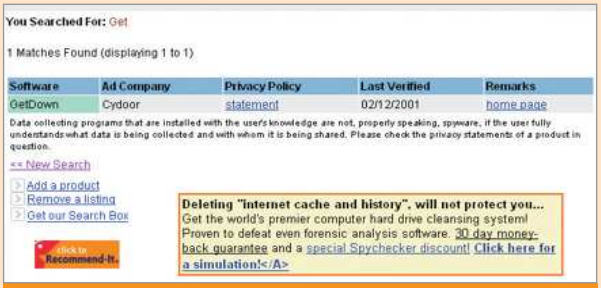
Diese Helfer sollten Sie installieren

SCHWIERIGKEIT: FÜR EINSTEIGER

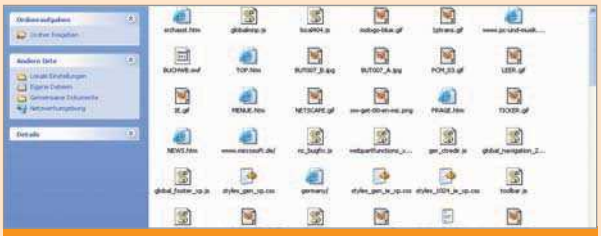
Um Spion-Software aufzuspüren und zu eliminieren, benötigen Sie nur ein Programm, das in der Lage ist, alle bekannten Spyware-Systeme auf der Festplatte zu identifizieren und zu löschen. Das Bekannteste ist „Ad-Aware“ von LavaSoft (www.lavasoft.de), das Spion-Software anhand einer Datenbank erkennt und diese Datenbank auf Wunsch auch auf dem allerneusten Stand hält. Die Anwendung von Ad-Aware ist völlig unkompliziert: Nach Anklicken eines Start-Buttons scannt das Programm alle vorhandenen Festplatten- oder sonstigen Laufwerke ab, zeigt gefundene Spion-Software in einer Liste und ermöglicht eine freie Auswahl der Einträge, die schlussendlich vom Datenträger entfernt werden sollen. Die Standard-Version von Ad-Aware ist kostenlos, eine Plus-Version mit mehr Funktionen kann über die Website bestellt werden.

Ist man nicht sicher, ob eine Shareware-Version mit Spion-Software (neben Radiate und Gator gibt es noch zig andere Firmen in den Vereinigten Staaten) „verseucht“ ist, lohnt sich ein Besuch auf der Website des „Spy-Checker“ (www.spychecker.com). Hier können Sie einen Online-Check vornehmen, indem Sie den Namen einer Software oder einen Teil davon in eine Datenbanksuche eingeben. Auf diese Weise bleiben Sie von Spion-Software zumindest zu 95 Prozent verschont.

JÜRGEN BORNGIESSER



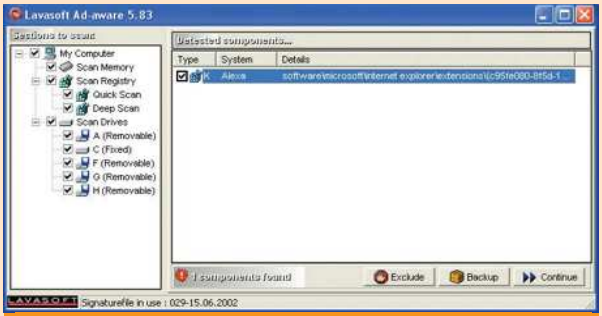
ONLINE-PRÜFER Auf www.spychecker.com können Sie online überprüfen, ob eine Software Spyware enthält, und es gibt Tipps, diese zu entfernen.



ABSTELLKAMMER Im temporären Speicher können sich Spion-Module, aber auch Banner mit direkten Links oder Web-Bugs verstecken.

WEB-BUG? GIF-Bilder mit weniger als 1 kByte Größe und unbekannter Bezeichnung lassen auf die Herkunft als Web-Bug schließen.

AUFPASSER Ad-Aware von LavaSoft ist das derzeit beste Programm für das Aufspüren und Eliminieren von Spion-Software auf dem PC.

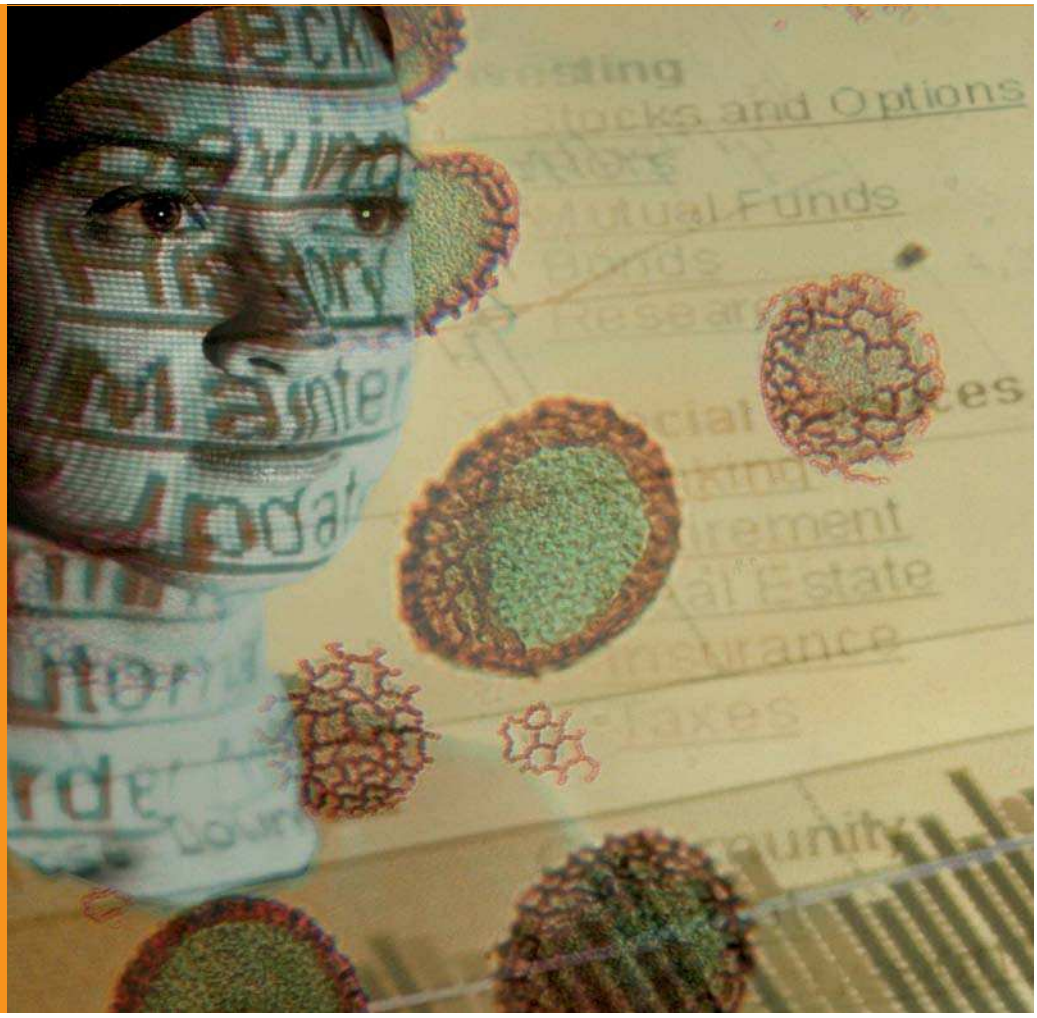


GEFUNDEN Hier ist es das Microsoft-eigene System „Alexa“, das nach jeder Windows-XP-Installation mit auf die Festplatte übertragen wird.

Makroviren bei Word und Excel

Nie wieder Love Letters?

Makroviren sind noch gar nicht so alt, aber schon eine schlimmere Plage als alle anderen Viren zusammengenommen. Dabei sind Abwehr und Schutz gar nicht so schwer.



Fast jeder Internetnutzer hat bereits unliebsame Bekanntschaft mit Makroviren geschlossen. Im günstigsten Fall hat er gar nichts davon mitbekommen, weil der Antivirenschutz optimal konfiguriert und auf dem neuesten Stand ist. Wer Glück hatte, verschob die E-Mail mit Attachment vom unbekannten Absender aus lauter Gewohnheit gleich in den Ordner „Gelöschte Nachrichten". Ohne Gunst und Glück dagegen sind alle Adressen aus dem Outlook-Express-Adressbuch mit genau der gleichen Nachricht und dem gleichen Inhalt an alle Adressaten versendet worden – der Virus hat sich weiterverbreitet. Word- und Excel-Dateien sind nicht nur infiziert, sondern eventuell sogar unbrauchbar – und das alles durch ein kleines Programm, dessen Ursprung vielleicht ein experimentierfreudiges Computer-Kid ist.

Die Ursache: Scriptsprachen

SCHWIERIGKEIT: FÜR EINSTEIGER

Mit der Einführung von „Microsoft Office" in Form der Textverarbeitung „Word" und der Tabellenkalkulation „Excel" wurden auch diverse Tools mitgeliefert, die den Umgang mit den beiden Office-Produkten vereinfachen sollten. Dazu gehört auch „VBA" („Visual Basic for Applications") und dessen Script-Ableger. In den Office-Produkten selbst wurde ein VBA-Makrosystem integriert, mit dem öfter wiederkehrende Befehlsstrukturen zu einem in der Applikation selbst ablaufenden „Makro" zusammengefasst werden konnten. Vereinfacht gesagt: Wurde zum Beispiel in „Word" ein Text auf bestimmte Weise in mehreren Durchläufen formatiert, so konnte dies nun durch die Aufzeichnung der Befehlssequenzen in einem Makro zusammengefasst und durch

WAS IST?

JavaScript
Spezielle Scriptsprache zur Unterstützung dynamischer Webinhalte

Wurm
Virus-Art, enthält einen speziellen Code, der in das PC-System eingeschleust wird

Makro
Zusammenfassung von Befehlsstrukturen, um Arbeitsgänge zusammenzufassen

Runtime-Modul
Ermöglicht es nicht selbstablaufenden Programmen, automatisch zu starten

Aufruf des Makros in einem Durchgang erledigt werden. Damit solche Makros funktionieren, muss der Rechner über die Applikation eine Reihe von Befehlssequenzen erhalten, die im Makro Schritt für Schritt abgearbeitet werden. Diese Befehle sind zum Beispiel in einer Scriptsprache wie VBScript festgeschrieben. Anders als bei weiteren Scriptsprachen hat man bei VBScript allerdings ein bisschen zu viel des Guten getan. So ist es möglich, über VBScript und VBA Systembefehle einzubauen, darunter auch das Schreiben und Löschen von Daten und Dateien. Auch das Formatieren eines Datenträgers ist – wenn auch mit einigen programmiertechnischen Verrenkungen – möglich. Und genau da fangen die Probleme an.

VBA und VBScript sind nämlich in der Lage, mit jedem Office-Programm zu kommunizieren, welches diese unterstützt. Dazu gehören zum Beispiel neben „Word“ und „Excel“ auch „Outlook“ und „Outlook Express“. Da beide Programme als E-Mail-Client fungieren und über ein eigenes Adressbuch mit gespeicherten Datensätzen verfügen, braucht man an dieser Stelle nur die entsprechenden Befehlssequenzen zusammenzulegen und bekommt so ein Programm, das Zugriff auf Systemressourcen erhält und selbstständig weitere Verbreitung findet – die besten Voraussetzungen für einen Virus.

Das Resultat: Makroviren

SCHWIERIGKEIT: FÜR EINSTEIGER

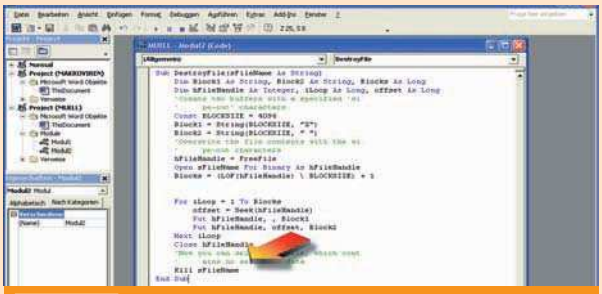
Ein Makrovirus ist ein Makroprogramm, dessen interne Befehlsstruktur darauf abzielt, Daten und Dateien zu löschen, zu manipulieren oder zu zerstören und gleichzeitig sich selbst zu verbreiten. Das bedeutet aber auch, dass der Virus nicht von sich aus aktiv werden kann. Er braucht zum Start ein ausführendes Programm, also Word, Excel oder ein Runtime-Modul. Anders gesagt: Jeder Makrovirus muss sein „Opfer“ dazu bringen, die entsprechende Applikation zu starten. Das geht allerdings recht schnell: Der Virusträger besteht aus einem Excel- oder Word-Dokument und wird als Attachment an die Mail angefügt. Der Betreff und der Inhalt der Mail müssen nun noch den Anreiz bieten, das Attachment zu öffnen, was meist durch einen Doppelklick geschieht. Wird die Datei nämlich nicht gespeichert, sondern gleich über den Doppelklick mit der entsprechenden Applikation ausgeführt, kann das Makro aktiv werden. Allerdings auch erst nach Bestätigen der unter Windows immerhin enthaltenen Sicherheitsabfrage.

Wenn Sie jetzt meinen, dies seien genug Hindernisse für Makroviren, dann liegen Sie allerdings falsch. Der Fall „Love Letter“ hat gezeigt, wie schnell sich solche Viren verbreiten können: Am 4. Mai 2000 wurden weltweit die Server des Internet durch eine Flut von E-Mails mit angehängter Datei lahm gelegt. Der Grund war ein kleines VBScript. Es kopierte sich durch das Adressbuch von Outlook Express und Outlook weiter, so dass die Verbreitung in rasender Geschwindigkeit stattfand. Daran war auch die Unvorsichtigkeit vieler User schuld, die den Betreff „ILOVEYOU“ zum Anlass nahmen, die eigentliche Virusdatei „LOVE-LETTER-FOR-YOU.TXT.vbs“ zu öffnen.

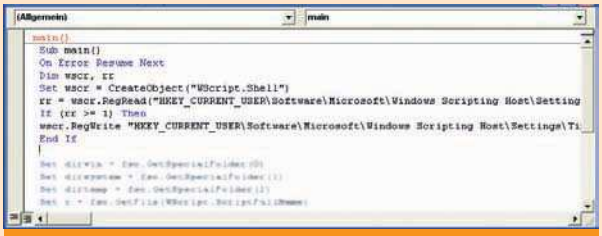
Gefahr: Windows blendet Datei-Endungen aus

SCHWIERIGKEIT: FÜR EINSTEIGER

Dass es Makroviren so leicht haben, liegt oft an den Benutzern, zum Teil aber auch an Windows selbst. Wenn Sie den Programmnamen aufmerksam lesen, fällt Ihnen auf, dass es „zwei“ Endungen gibt: .TXT und .VBS. Windows zeigt Datei-Endungen bekannter Programme oder Dateien nicht an, deshalb erscheint nicht die VBS-Endung, die auf ein VBScript hinweist, sondern eine Endung „.TXT“, die eine Textdatei sein soll. Durch das doppelte Anklicken der Datei wird diese dann nicht vom Editor geöffnet, sondern von der Applikation. Das Ausblenden der Datei-Endungen kann man unterbinden. Dazu müssen Sie in das Menü „Extras“ eines geöffneten Windows-Ordners und dort in die Registerkarte „Ansicht“ gehen. Wenn Sie hier vor



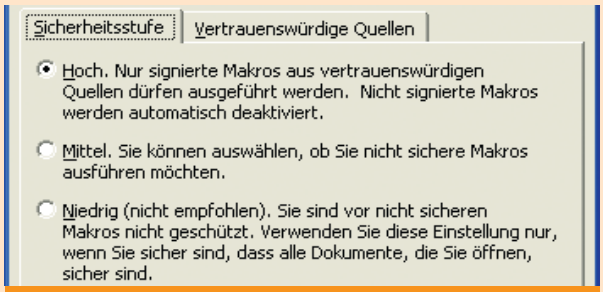
GEFÄHRLICH Der Visual Basic Script-Editor von Word und ein VBScript zum Löschen einer frei bestimmbaren Datei, durch einen „Kill“-Befehl.



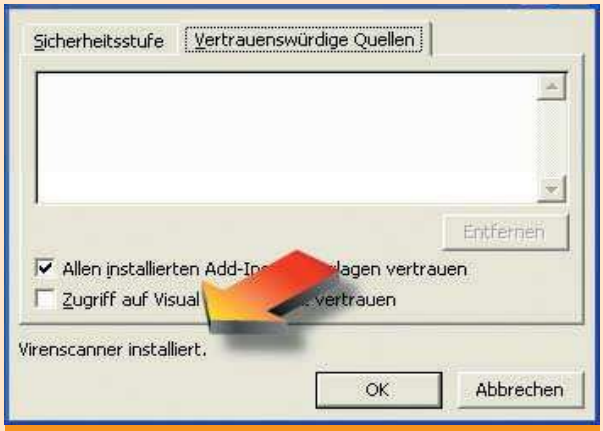
LIEBESGRÜSSE Diese Codezeilen gehören zum Love-Letter-Virus. Der Befehl „CreateObject (WScript.Shell)“ öffnet Tür und Tor zu Systemdateien.

DATEI-ENDUNG Unbedingt Datei-Endungen korrekt anzeigen lassen. So vermeidet man das Einschleusen versteckter Scripte.

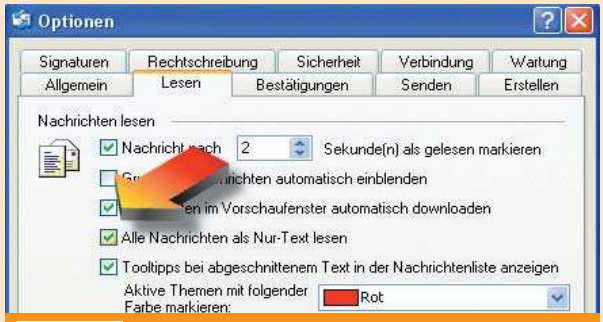
MAKROSCHUTZ In den Optionen von Word verbirgt sich der Makroschutz. Standardmäßig ist eine hohe Sicherheit voreingestellt.



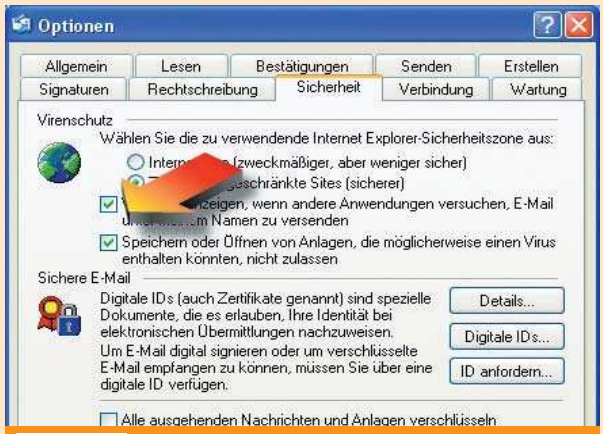
MAKROSICHERHEIT Schauen Sie nach, ob die Schutzeinstellungen der Word-Makros auf „Hoch" eingestellt sind. Falls nicht, holen Sie es bitte nach.



VERTRAUEN Im Ordner „Sicherheit" können Sie „Vertrauenswürdige" Makrodateien festlegen, die ohne Rückfrage ausgeführt werden dürfen.



HTML-KILLER In Outlook Express kann festgelegt werden, dass Nachrichten nur in Textform ohne HTML-Umgebung dargestellt werden sollen.



UNGEÖFFNET In den Einstellungen können Sie über „Speichern oder Öffnen von Anlagen ..." verhindern, dass Attachments aktiv ausgeführt werden.

dem Eintrag „Erweiterungen von bekannten Dateitypen ausblenden" das Häkchen entfernen, werden die Endungen aller Dateien richtig angezeigt. Erst dann sehen Sie, ob es wirklich einen Text im Anhang gibt, ob das .DOC am Ende wirklich auf ein Dokument hinweist oder ob es sich um VB-Programmzeilen handelt.

Trotz allem werden Makroviren immer wieder verschickt – und sie haben immer wieder Erfolg. Denn die Virenprogrammierer nutzen eine menschliche Schwäche aus: die Neugier. Mit verheißungsvollen Bezeichnungen wird sie geweckt und man ist bloß noch einen Doppelklick von der Virus-Infektion entfernt. Die verräterischen Endungen „.VBS", „.DOC" oder „.XLS" bleiben nämlich häufig leider unbemerkt.

Schutzmaßnahme: Makroschutz aktivieren.

SCHWIERIGKEIT: FÜR EINSTEIGER

Die meisten guten Virenscanner können Makroviren inzwischen einwandfrei erkennen und verfügen auch über einen E-Mail-Schutz, der die Nachrichten direkt nach dem Laden vom Server auf Viren überprüfen. Aber selbst ohne Viruskiller ist ein Schutz vor Makroviren problemlos möglich, wenn ein paar wichtige Regeln eingehalten werden.

Die erste lautet ganz einfach: Öffnen Sie auf gar keinen Fall Nachrichten unbekannter Herkunft, die Attachments beinhalten, mit Doppelklick. Und sollte es Ihnen dennoch passieren, dann stoppen Sie dies spätestens dann, wenn ein Makro zur Ausführung kommen soll. In Word zum Beispiel findet sich im Menü „Extras" und unter dem Menüpunkt „Optionen" die Registerkarte „Sicherheit", in der sich der Eintrag „Makrosicherheit" verbirgt. Die Einstellung „Hoch" ist hier unbedingt Pflicht. Die zweite Regel ist sogar noch einfacher: Installieren Sie unbedingt alle Updates zu Ihrer Windows-Software. Nur so werden Sicherheitslücken geschlossen und Fehler, die Makroviren ausnutzen könnten, entfernt.

Problem HTML-Mails

SCHWIERIGKEIT: FÜR EINSTEIGER

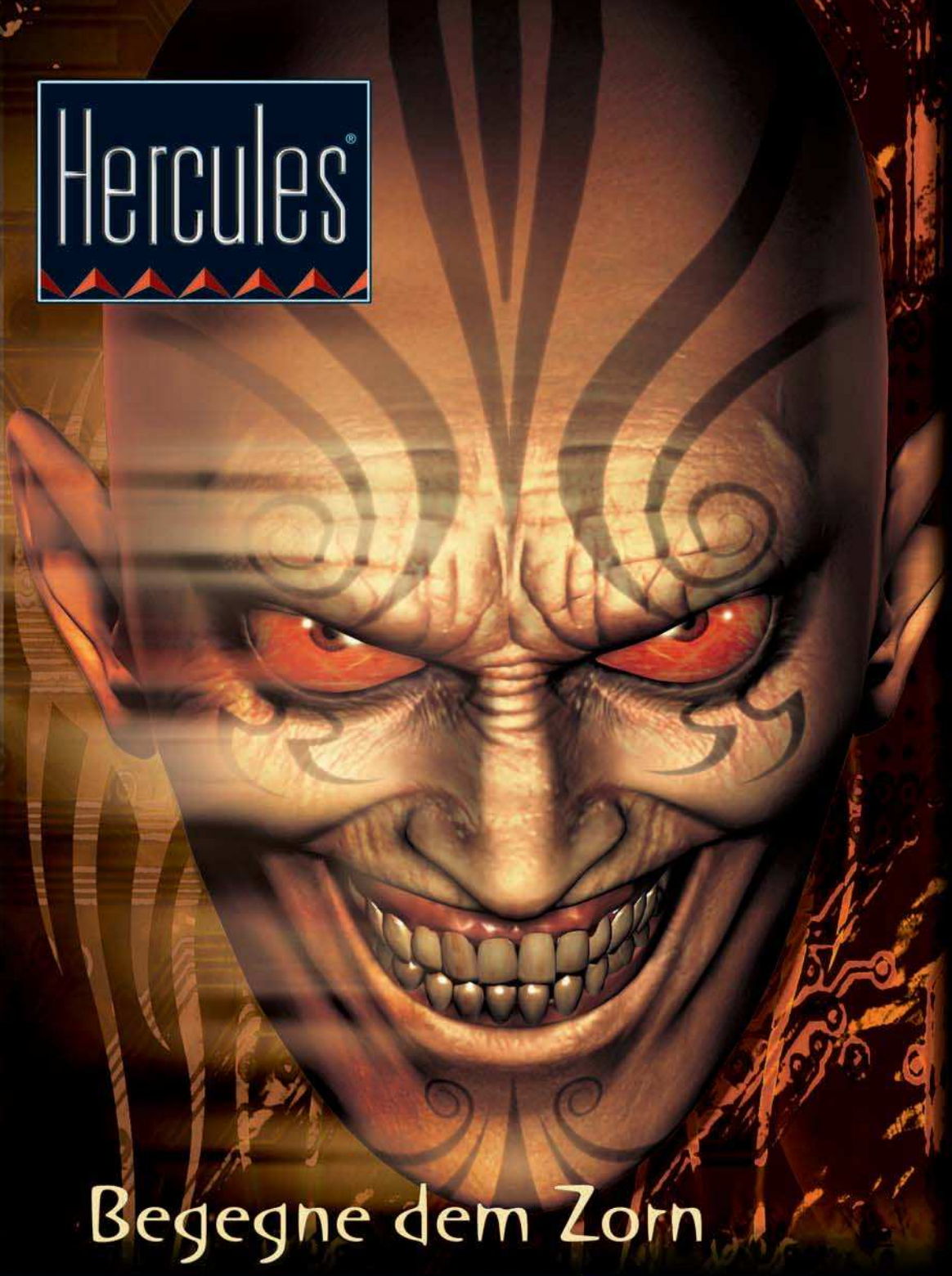
Noch gefährlicher als reine Makroviren sind HTML-Würmer, die mit Makroviren verkettet sind. Ein solcher Kombi-Viruswurm nutzt eine Sicherheitslücke unter Outlook und Outlook Express aus. Er enthält ein Attachment, ist gleichzeitig aber im Code einer HTML-Nachricht enthalten. Wenn diese HTML-Nachricht geöffnet wird, versucht Outlook, den Inhalt in Form von HTML-Code nachzubilden. Dabei wird ein Script gestartet, das automatisch das Attachment öffnet und zur Ausführung bringt. Der Wurm spioniert danach nicht nur Benutzerdaten aus, er öffnet auch noch den TCP-Port 36794, über den Firewall- und Antiviren-Software Daten übermitteln. Findet er derartige aktive Software, versucht er diese zu überlisten und „blind" zu schalten.

Outlook Express bietet in den neuen Versionen unter Windows XP einen entsprechenden Schutz vor solchen Würmern an. Im Menü „Extras" befindet sich unter „Optionen" in der Registerkarte „Lesen" der Eintrag „Alle Nachrichten als Nur-Text lesen". Standardmäßig ist die Funktion ausgeblendet. Wenn Sie hier die Marke setzen, wird ab sofort jede Nachricht wie normaler Text behandelt, die HTML-Codes werden nicht mehr in die Render-Darstellung übernommen und enthaltener Script-Code, zum Beispiel JavaScript oder VBScript, kommt nicht mehr zur Ausführung.

In der Registerkarte „Sicherheit" ist der Menüpunkt „Speichern oder Öffnen von Anlagen, die möglicherweise einen Virus enthalten könnten, nicht zulassen" standardmäßig aktiviert. Damit sind Attachments nicht mehr direkt aktivierbar. Nachteil: Auch erwünschte Attachments liegen fest. Es gibt allerdings wieder einen kleinen Trick, diesen Schutz zu umgehen: Wenn Sie auf den Button „Weiterleiten" klicken, wird die Nachricht mitsamt Attachment als neue Mail angezeigt und alle Attachments sind wieder frei zugänglich.

JÜRGEN BORNGIESSER

Hercules®



Begegne dem Zorn des Propheten!

3D PROPHET 9500 PRO

AGP
DirectX® 9 Hardware-Beschleuniger
275 MHz Core/ 270 MHz RAM

3D PROPHET 9700

AGP
DirectX® 9 Hardware-Beschleuniger
275 MHz Core/ 270 MHz DDR RAM

Enthält die englische Vollversion von
No One Lives Forever™ 2
A SPY IN H.A.R.M.'S WAY™

PROPHETVIEW 720

Das Multimedia-TFT-Display im Designgehäuse. Schnelles 15" TFT zur flüssigen Darstellung von DVD-Videos und Spielen.

Enthält die englische Vollversion von
The Elder Scrolls III
MORROWIND

POWERED BY ATi RADEON 9700 PRO™

3D PROPHET 9700 PRO

- Unglaublich schnelles Hardcore-Board mit extrem hohen Frameraten in 3D-Spielen
- Microsoft DirectX®9 Plattform & ultra-realistisches 3D
- Hochqualitative Hercules Produktionsstandards
  - Kupferkühler: optimale Kühlung für mehr Stabilität
- Im Bundle: Die englische Vollversion des preisgekrönten The Elder Scrolls III: Morrowind™

www.hercules.de

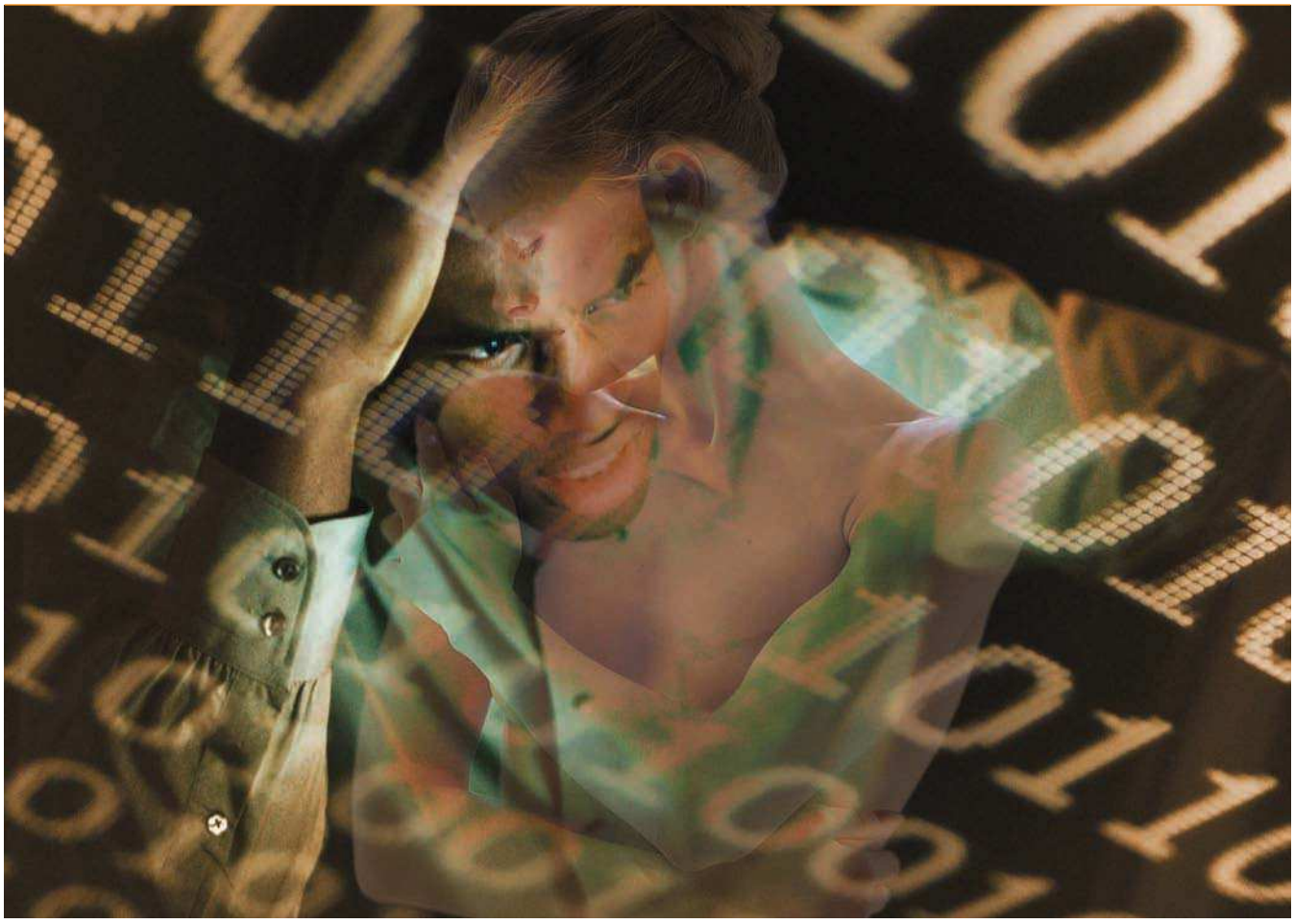
www.shop-hercules.de

erhältlich bei:
expert
MediaMarkt
K&M Elektronik
SATURN

© Guillemot Corporation 2002. All trademarks are the property of their respective owners. Illustrations not binding. Contens, designs and specifications are subject to change without notice and may vary from one country to another. Original 3D model for 3D Prophet 9000 series created by Franck Massiou. Morrowind:©2002 Bethesda Softworks Inc., a ZeniMax Media company. The Elder Scrolls, Morrowind, Bethesda Softworks, ZeniMax and their respective logos are registered trademarks or trademarks of ZeniMax Media Inc. in the United States and/or other countries. Distributed by Ubi Soft Entertainment. All Rights Reserved.

0190-Dialer im Visier

Schluss mit der Abzocke!



Dialer sind zu einer echten Plage geworden. Einmal installiert, treiben sie die Telefonrechnung in die Höhe und den Internetnutzer in den Wahnsinn. Doch es gibt Schutzmaßnahmen, die greifen.

Einen Dialer installiert zu bekommen, geht schneller, als Sie denken. Selbst Profis ist es schon passiert – kaum wurde im Internet ein „Submit"-Button zu viel angeklickt, schon startet Windows durch und installiert ein neues Anwahlsystem, das über eine teure 0190-Nummer Verbindung aufnimmt und pro Minute immense Gebühren verschlingt. Und wer richtig Pech hat, merkt es nicht einmal, dass ein Dialer im Hintergrund arbeitet, – oder zumindest erst dann, wenn die aktuelle Telefonrechnung auf den Tisch flattert. Und genau dann fangen die Probleme richtig an: Soll man die Summe zahlen? Soll man nicht? Was passiert überhaupt, wenn man sich weigert? Doch so weit sollte es erst gar nicht kommen.

Hinter dem Namen „Dialer" versteckt sich ein kleines Programm, das sich unter Umgehung von Sicherheitsabfragen – oder durch Verschleiern derselben – auf dem lokalen PC einnistet und eine neue Verbindung zu Telefondiensten über das Internet einrichtet. Oft geschieht dies durch einfachen Austausch der bestehenden Nutzer- und Anwahldaten, sogar ohne dass es der Benutzer anfangs merkt. Dialer sind in der letzten Zeit zu einer größeren Gefahr geworden als so mancher Virus. Bei einem Virus wird vielleicht das Rechnersystem beeinträchtigt, im schlimmsten Fall sind wichtige Daten verschwunden. Bei einem Dialer dagegen wächst die Summe der Telefongebühren dermaßen steil an, dass am Ende des Berechnungszeitraums auf der Telefonrechnung nicht selten Tausende von Euro auf der

WAS IST?

Dialer
Programm zur direkten Anwahl von Telefonnummern und gebührenpflichtigen Diensten

DSL
Digital Subscriber Line; digitale Breitband-Netzwerkverbindung über das Telefonnetz der Telekom

ActiveX-Control
Tool zur dynamischen Steuerung von Webseiten; kann Browser und Windows von „außen" aktivieren

Plug-In
Zusätzliches Programm für den Internet-Browser, um spezielle Inhalte anzuzeigen

Soll-Seite stehen. Dabei besteht das größte Problem darin, dass man nur schwer beweisen kann, den Dienst unwissentlich in Anspruch genommen zu haben.

Windows ist beliebtestes Dialer-Opfer

SCHWIERIGKEIT: FÜR EINSTEIGER

Windows-PCs sind die hauptsächlichen Opfer der Dialer-Technik. Das liegt vor allem an der verwendeten Einwahltechnik für Internetzugänge: Bei Modem- (analog) oder ISDN-Zugängen (digital) läuft die Einwahl über das DFÜ-Netzwerk. Jeder DFÜ-Netzwerkeintrag enthält eine Anwahlnummer sowie die notwendigen Informationen zur verwendeten Hardware (Modem oder ISDN-Karte/-Anlage). Die entsprechenden Treiber, bei Modem normale Geräte-Treiber, bei ISDN zusätzlich CAPI („Common Application Programming Interface“, spezielle Schnittstelle für digitale Übermittlungsgeräte) oder NDIS („Network Driver InterfaceSpecification“, spezielle Netzwerktreiber für ISDN-Anschlussgeräte), werden so im Windows-System integriert, dass die Anwahl direkt aus Applikationen wie Browser oder E-Mail-Client heraus funktioniert. Wird ein Programm installiert, eben jener Dialer, der die Anwahleinstellungen selbstständig gegen neue austauscht, wählt Windows ab dem installierten Zeitpunkt mit den neuen Einstellungen. Bei der DSL-Technik ist die Gefahr durch einen Dialer nicht gegeben: Da hierbei durch eine spezielle Treibertechnik ein dauerhafter Netzwerkanschluss ohne Anwahl besteht, kann ein Dialer nicht greifen. Es sei denn, es befindet sich zusätzlich zur DSL-Hardware noch Modem- oder ISDN-Hard- und -Software im Rechner.

Was ist eigentlich ein Dialer?

SCHWIERIGKEIT: FÜR EINSTEIGER

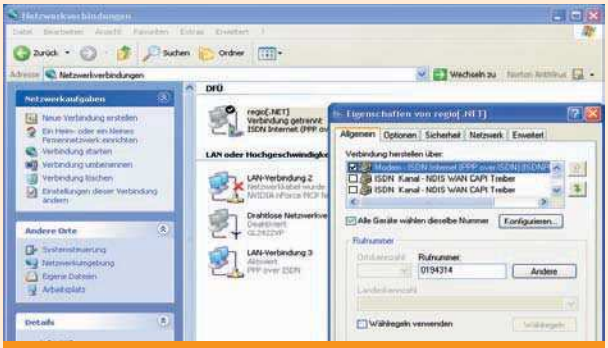
Ein Dialer ist eigentlich ein Verbindungsprogramm für kostenpflichtige Dienste. Er soll dem Benutzer den Zugang erleichtern und ihn ohne umständliche Anmeldungen und Einrichtungen direkt auf den Dienst lenken. So könnte man zum Beispiel kostenpflichtige Programm-Downloads organisieren, die Abrechnung geschieht ohne Kreditkartenabrechnung oder separate Rechnungsstellung einfach mit der Telefonrechnung. Zu diesem Zweck werden in Deutschland so genannte „Mehrwertnummern“ mit einer 0190er-Vorwahl vergeben. Diese Vorwahlen werden von Providern vertrieben und können von Dienstleistern angemietet werden. Die Schwachstelle: Die Gebühren können bei 0190-0-Vorwahlen sowie bei 0191-0194 frei bestimmt werden. Installiert sich ein Dialer-Programm mit der Anwahl einer solchen Nummer, können die Minutenpreise für die Verbindung entsprechend hoch sein. Da die Vorwahlnummern nicht eindeutig einem „Besitzer“ zugeordnet werden müssen, sondern durch weitere Vermietungsverträge verfügbar sind, lässt sich oft nicht eindeutig festlegen, wer an diesen Nummern nun eigentlich verdient – was zum Problem werden kann, wenn es wegen einer viel zu hohen Gebührenabrechnung zum Rechtsstreit kommt. Seit dem 1.1.2003 werden nun auch 0900-Vorwahlen vergeben. Diese sind nicht tarifgebunden, das heißt, dass auch hier die Gebühren frei festlegbar sind. Zwar soll ein Limit für die Gebühren nach oben hin festgesetzt werden, allerdings ist dies zurzeit noch nicht geschehen. Die neuen 0900-Vorwahlen sind streng nach Dienstanbieter geordnet und sollen die bisherigen 0190-Nummern ablösen. Bis zum Jahr 2005 bleiben diese allerdings noch bestehen – und damit die Gefahr der Gebührenfallen. Die Telekom will aber inzwischen nicht mehr die Inkassozahlung für gebührenpflichtige 0190er-Dienste übernehmen. Das wiederum bedeutet, dass der gebührenpflichtige Dienst seine Rechnungsforderung direkt an den „Kunden“ stellen muss. Das wiederum könnte bedeuten, dass viele unseriöse Anbieter ihr „Angebot“ nicht mehr so einfach an den „Kunden“ bringen könnten.

Seriöse Anbieter

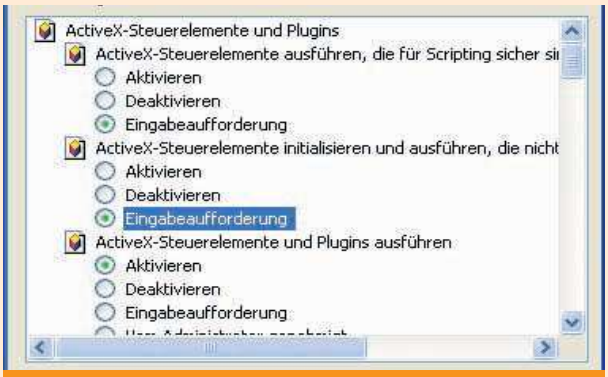
SCHWIERIGKEIT: FÜR EINSTEIGER

Wer im Internet auf kostenpflichtige Dienste trifft, hat zwei

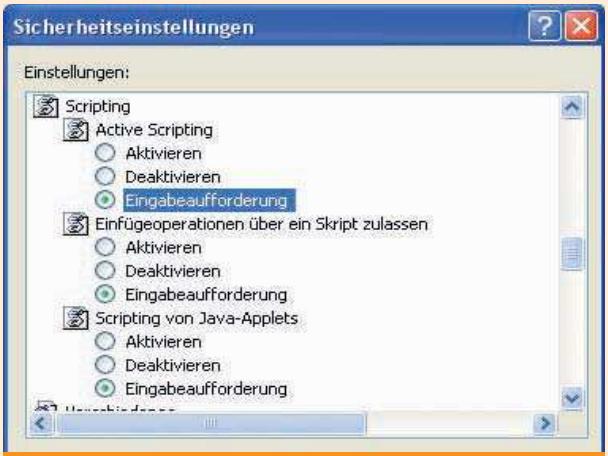
SO GEHT'S AUCH Hier wird auf Benutzung eines Dialers explizit hingewiesen. Gebühren sowie Vertragspartner sind für den Benutzer klar erkennbar.



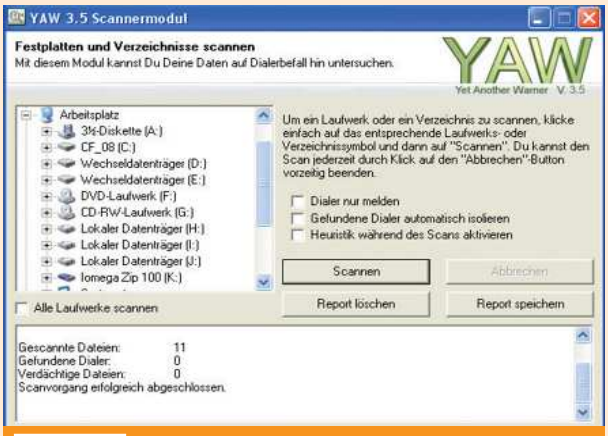
DFÜ-NETZWERK Unter Windows XP werden die DFÜ-Netzwerkeinstellungen nicht nur besser angezeigt, sie lassen sich auch besser konfigurieren.



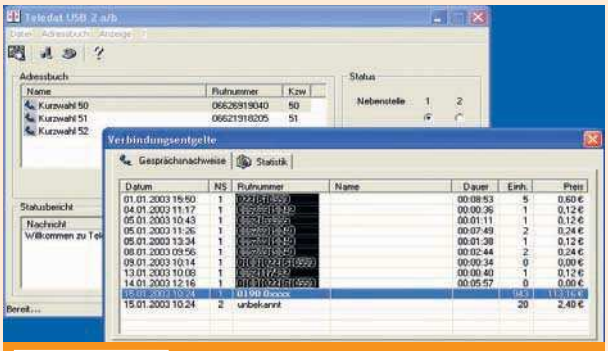
ACTIVEX Um automatisch installierten Dialern vorzubeugen, sollten Sie in den Internetoptionen die ActiveX-Kontrollen am besten ganz deaktivieren.



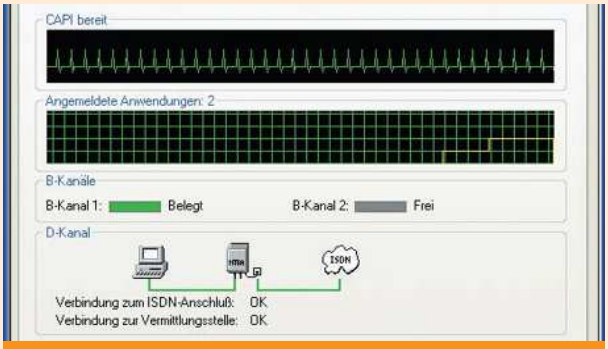
SCRIPT-EINSCHRÄNKUNG Um automatischen Vorgängen auf Webseiten entgegenzuwirken, sollten Sie das Starten von Script-Dateien einschränken.



AKTIVSCHUTZ Dialerschutzprogramme wie YAW scannen die Laufwerke auf Dialer-Einträge und isolieren oder löschen entsprechende Einträge.



GEBÜHRENANZEIGE Viele ISDN-Anlagen bieten die Möglichkeit, die Gebühren genau anhand der geführten Telefongespräche zu protokollieren.



ISDN-SCHUTZ Um CAPI-Dialer zu erkennen, sollte ein ISDN-Kanalmonitor zum Einsatz kommen, der Verbindungen über ISDN-Kanäle anzeigt.

INTERNET-HILFE Die Webseiten von Dialerschutz.de liefern viele zusätzliche Informationen rund um das Thema Dialer, Abwehr und Rechtsmittel.

Chancen: Die erste ist bei seriösen Anbietern zu finden, die den Dialer ankündigen und zum freiwilligen Download bereithalten, zudem eine genaue Angabe über die anfallenden Gebühren anzeigen und dem Benutzer die volle Kontrolle über den Dialer geben. In diesem Fall weiß jeder Nutzer genau, wie der Dialer funktioniert und wie man ihn einsetzt. Die zweite Chance ist die wesentlich schlechtere: Der Dialer wird verschleiert installiert, indem man dem Benutzer vorgaukelt, nur ein wichtiges Zugangssystem einzurichten, es gibt keine Informationen über die anfallenden Gebühren, außerdem ist der Betreiber des Dialers nicht erkennbar. Diese dubiosen Angebote finden sich meist bei Servern mit illegalen Angeboten im Internet. Es gibt allerdings Methoden, diese Gefahren gleich zu Anfang zu erkennen.

Die Wichtigste zuerst: Schauen Sie genau nach, was auf der Seite zu finden ist, und machen Sie einen Screenshot (Taste [Druck], dann „Einfügen“ in ein Grafikprogramm). Wenn ein automatisch installierter Dialer vorliegt, können Sie später zumindest auf die Seite hinweisen, auf der Sie sich das Programm eingefangen haben. Denn viele der Angebotsseiten wechseln oft den Server und die Adresse, so dass eine spätere Rückverfolgung kaum möglich ist.

Grundsätzliche Maßnahmen gegen Dialer

SCHWIERIGKEIT: FÜR FORTGESCHRITTENE

Installieren Sie am besten eines der gängigen Anti-Dialer-Tools wie „YAW“ (Yet Another Warner, www.yaw.at) oder „0190-Warner“. Informationen zum Thema Dialer und Abwehr finden Sie im Internet vor allem unter der Adresse von „Dialerschutz.de“ (www.dialerschutz.de). Dort gibt es nicht nur sehr viele Informationen zu Dialern und deren Funktionen oder Auswirkungen, sondern auch viele Tools gegen Dialer sowie Hilfestellungen für den Fall, dass ein Dialer zugeschlagen hat. So wurden bei „Dialerschutz“ Gerichtsurteile oder Rechtshinweise zusammengetragen, die darüber Aufschluss geben, wie das Thema Dialer bei Streitfällen gehandhabt wird. Wenn Sie im Web surfen und Seiten mit nicht regulären Inhalten besuchen, müssen Sie sich der Gefahr bewusst sein, dass solche Inhalte oft nur durch gebührenpflichtige Wählprogramme genutzt werden können. Sofern Sie gesondert auf das Angebot, die Gebühren sowie den zustande kommenden Vertrag hingewiesen werden, handelt es sich in der Regel um ein seriöses Angebot. Finden Sie jedoch plötzlich Download-Anfragen oder ein Programm versucht automatisch, ein „Plug-In“ für Ihren Browser zu aktivieren, sollten Sie die Verbindung sofort abbrechen und die Seite verlassen. Versuchen Sie nicht, den Download zu deaktivieren, meist sind die entsprechenden Windows-Funktionen sowieso abgeschaltet, so dass eine Reaktion zu spät kommt. Sind Sie nicht sicher, ob ein Dialer tatsächlich installiert wurde, installieren Sie eines der Dialerschutz-Tools und scannen Sie Ihre lokalen Datenträger auf verdächtige Eintragungen. Inspizieren Sie auch den DFÜ-Netzwerkeintrag auf sichtbare Änderungen der Einwahl.

Vorsicht bei Eingaben auf Webseiten

SCHWIERIGKEIT: FÜR EINSTEIGER

Ein immer wieder auftauchendes Problem sind die ActiveX-Kontrollen innerhalb von HTML-Seiten. Das von Microsoft entwickelte Pendant zu JavaScript verfügt von Haus aus über besondere Zugriffstechniken auf die Windows-Ressourcen und lässt es relativ leicht zu, einen Dialer per Kontrollmechanismus automatisch als Download zu aktivieren und eine Installationsroutine zu starten. Vor allem auf Webseiten mit illegalen Inhalten werden solche Installationsmechanismen gerne genutzt, weil die Betreiber der Website dadurch ihre Server finanzieren. Um solchen Attacke vorzubeugen, sollten Sie in den Internetoptionen die unter den „Sicherheitseinstellungen“ befindlichen Einträge für ActiveX-Kontrollen von „Aktivieren“ auf „Deaktivieren“ oder zumindest auf „Eingabeaufforderung“ abändern. Wenn der Browser auf

ActiveX-Kontrollen trifft, werden diese nicht mehr automatisch gestartet, sondern im günstigsten Fall abgeblockt oder zumindest dem Benutzer angezeigt. Das Gleiche trifft für alle Einträge unter „Scripting“ zu, damit lassen sich zum Beispiel Java-Applets, die durch JavaScript oder Visual-Basic-Scripts (VBS) gestartet werden, ebenfalls verhindern.

E-Mails mit verfänglichen Inhalten beachten

SCHWIERIGKEIT: FÜR EINSTEIGER

In letzter Zeit kommt es häufig vor, dass Spam-Mails (unverlangte Werbe-E-Mails) mit Inhalten wie „kostengünstiger Internetzugang“ oder Ähnliches von Quellen verschickt werden, die keinerlei Rückschlüsse auf den tatsächlichen Absender erlauben. Diese Mails enthalten Attachments, die angeblich ein Zusatz-Tool enthalten, mit dem sich der Provider kostengünstiger anwählen lässt. In Wirklichkeit jedoch wird die Nummer des Providers über einen 0190-Anbieter geschaltet, der dann weitaus höhere Gebühren verlangt. Die zweite E-Mail bezieht sich auf einen angeblich „gecrackten“ Dialer, der nun kostenlosen Zugang auf Webseiten mit „eindeutig zweideutigem“ Inhalt verspricht. Tatsächlich ist der Dialer jedoch weder „gecrackt“ noch kostenlos, er verbindet über die teure 0190-Nummer mit dem entsprechenden Dienst und lässt sich zudem auch nur schwer wieder aus dem System entfernen. Daher unser Tipp: Solche E-Mails bitte schnellst möglich in den Ordner für „gelöschte Nachrichten“ weiterleiten.

CAPI-Dialer erkennen und entfernen

SCHWIERIGKEIT: FORTGESCHRITTENE

ISDN-Benutzer sind einer weiteren Gefahr durch Dialer ausgesetzt, den so genannten CAPI- oder TAPI-Dialern. Dabei handelt es sich um kleine Programme, die eine Art „Netzwerk“-Zugang installieren und direkt auf den CAPI-Treiber einer ISDN-Karte oder -Anlage zugreifen. Diese CAPI- oder TAPI-Installationen werden von Dialerschutz-Tools nicht immer erkannt und sind auch nicht auf dem Bildschirm aktiv oder im DFÜ-Netzwerk erkennbar.

Hier hilft nur das Installieren eines Tools zur Beobachtung der einzelnen ISDN-Kanäle wie zum Beispiel „ISDN-Watch“, das Sie unter der Adresse www.isdnwatch.co.uk herunterladen können. Ist eine andere Karte oder Anlage installiert, lohnt es sich, ein solches Tool extern zu installieren. Hier empfiehlt sich der äußerst zuverlässige „PowerISDNMonitor“ von Thilo Brandt (www.powerisdnmonitor.de), ein kostenloses Tool, das neben der Kanalüberwachung auch noch viele andere nützliche Eigenschaften wie MSN- und Anruferüberwachung bietet. Zeigt die Kanalüberwachung an, dass ISDN-Kanäle automatisch belegt werden, ohne dass Telefon oder DFÜ-Netzwerk aktiviert wurden, sollten Sie sofort die Verbindung beenden und die Autostart-Einträge sowie die Registry unter Windows überprüfen. Meist lassen sich Einträge anhand der Wählnummer (nach 019xxx-Nummern suchen) identifizieren.

JÜRGEN BORNGIESSER

Hagen Hild

Beruf:
Rechtsanwalt

Aufgabe:
Spezialist für Internetrecht

Tätigkeit:
Herr Hild aus Augsburg betreibt unter anderem die Website www.kanzlei.biz und betreut die Internetseiten von www.dialerschutz.de.

„Setzen Sie sich zur Wehr!“

Wollen Sie gegen Dialer-Betrüger vorgehen, ist es wichtig, alle Beweise aufzuheben.

Wann muss ich für die Gebühren eines über eine 0190er- oder ähnliche Nummer geschalteten kostenpflichtigen Mehrwertdienstes aufkommen und wann nicht?
Wer einen Vertrag über eine Leistung durch eine Mehrwertdienstnummer geschlossen hat und sich damit bewusst ins Internet eingewählt hat, muss auch für die Gebühren aufkommen. Wird ein Dialer aber ohne Kenntnis und Einwilligung des Nutzers auf dessen Rechner installiert, erfährt der Nutzer hiervon meist erst durch die Telefonrechnung und ist erst mal natürlich nicht gewillt, für diesen ungewollten Dienst zu zahlen. Die rechtliche Situation ist kompliziert (...) Bisher wurde noch nicht höchstrichterlich entschieden, ob der Netzbetreiber im Fall einer unbewussten Dialer-Einwahl einen Anspruch auf Zahlung der Gebühren hat.

Wie kann ich beweisen, dass ein kostenpflichtiger Mehrwertdienst ohne mein eigenes Wissen und Zutun aktiviert wurde?
In erster Linie gilt es, den Dialer auf dem Rechner zu finden, unschädlich zu machen und zu sichern. In keinem Fall sollte der Dialer gelöscht werden oder die Festplatte formatiert werden, da sonst Beweise vernichtet sind. Von der Webseite, von der Sie den Dialer haben sowie vom eigenen Rechner, können Screenshots als Beweise angefertigt werden. Da eine Dialer-Installation und -Einwahl ohne Einwilligung des Nutzers strafbar ist, kann Strafanzeige bei der Polizei erstattet werden.

Was kann passieren, wenn ich die Gebühren eines Mehrwertdienstes nicht bezahle?
Das Verfahren der Telekommunikationsunternehmen läuft meist immer gleich ab: Zahlungsaufforderung des Netzbetreibers, Mahnungen, Zahlungsaufforderungen des Mehrwertdienst-Rufnummernbetreibers, Mahnungen, Inkasso-Unternehmen, Schreiben des Rechtsanwalts, Mahnbescheid, Gerichtsverfahren. Die Telekommunikationsanbieter arbeiten in der Regel mit vorgefertigten Standardschreiben und üben gezielt Druck auf den nicht Zahlungswilligen aus. Zu Gerichtsverfahren kommt es kaum. Wird in einem Gerichtsverfahren festgestellt, dass der Zahlungsanspruch berechtigt ist, hat der Nutzer diese Kosten zu tragen, andernfalls wird der Anspruch abgewiesen und der Kläger hat diese Kosten selbst zu tragen.

Welche rechtlichen Möglichkeiten habe ich, um gegen unberechtigte Ansprüche solcher Dienstanbieter vorzugehen?
Die Dialer-Anbieter setzen darauf, dass viele Geschädigte die Forderung einfach bezahlen. Ich kann den Geschädigten deshalb nur raten, sich zur Wehr zu setzen. Dazu sollten Geschädigte beim Netzanbieter Einwendungen gegen die angeblich angewählten Verbindungen erheben. Wer keinen Einzelverbindungsnachweis hat, sollte diesen unverzüglich anfordern. Der Anbieter muss auch die vollständige 0190er-Telefonnummer des Diensteanbieters mitteilen. Will das Telekommunikationsunternehmen seine Forderung durchsetzen, muss dieses klagen. Spätestens beim Mahnbescheid oder einer Klage sollte ein Anwalt mit Schwerpunkt Internetrecht hinzugezogen werden. Der Geschädigte kann auch selbst aktiv werden und negative Feststellungsklage erheben, dass der Anspruch nicht besteht. Dann muss das Telekommunikationsunternehmen vor Gericht beweisen, dass doch ein Anspruch besteht.

Alternatives Filesharing

Ins Netz gegangen

Dateitauschprogramme haben den Hauch des Illegalen. Wir zeigen Ihnen sinnvolle, legale Anwendungsmöglichkeiten. Damit auch Sie die Vorteile des dezentralen Konzeptes nutzen können.

Jeder von uns kennt die Situation: Ein Softwarehaus veröffentlicht eine neue Version ihres begehrten Benchmarks, einen megabytestarken Patch, die neue *UT 2003*-Demo oder gleich ganze Service Packs. Kaum ist die Pressemitteilung draußen, schon geht auf dem Download-Server nichts mehr. Ein anderes gutes Beispiel sind aktuelle Treiber. Manchmal können Sie nicht mal die Startseite von Ati aufrufen, weil viel zu viele Anwender versuchen, den neuen Catalyst-Treiber zu laden. Doch was kann man tun? Sie könnten zum Beispiel auf dem heimischen Rechner ein Verzeichnis mit allen wichtigen Treibern, Tools oder Updates anlegen. Alle anderen Anwender hätten so immer Zugriff darauf und müssten nicht erst dutzende Webseiten absurfen. Umgekehrt könnten Sie von den Daten anderer Nutzer profitieren und den Datenstau umfahren. Weiterer Vorteil: Je mehr Anwender eine Datei herunterladen, desto mehr Downloadquellen entstehen, die Datenübertragung wird schneller. Im herkömmlichen Internet würde der Download einer Datei dagegen umso langsamer, je mehr Anwender darauf zugreifen wollen. Genau hier liegt die Stärke der modernen Dateitauschprogramme.

Neben zahlreichen Tauschprogrammen wie Winmx, Kazaa oder Bearshare ist Edonkey am besten frequentiert. Jede Datei im Edonkey-Netzwerk, ob Patch oder Treiber, hat eine eindeutige Kennung. Stellt der Client nun fest, dass das gewünschte File nicht nur einmal vorhanden ist, setzt er alle anderen Quellen ebenfalls automatisch in die Downloadliste. Edonkey kann eine einzelne Datei stückweise von mehreren Anwendern gleichzeitig laden. Geht ein Nutzer offline, fällt das kaum ins Gewicht, sofern genügend andere noch online sind, von wo sich der Client das fehlende Teil ebenfalls holen kann. Gehen Sie selbst offline, ehe der eigene Download fertig ist, wird dieser bei der nächsten Einwahl fortge-

WAS IST?

Client
Ein Client ist ein Programm beziehungsweise eine Anwendung, die Dienste eines Servers in Anspruch nimmt und beispielsweise E-Mails von einem Server abruft.

Peer-to-Peer-Netzwerk
Nicht-hierarchisches Netz, in dem die verbundenen Rechner stets gleichberechtigten Zugriff auf die anderen PCs des Netzes haben. Es gibt keinen Server oder Client.

Server
Bezeichnung für den zentralen Computer eines Netzwerks, der seine Leistungen und Daten den am Netzwerk teilnehmenden Computern (Client) zur Verfügung stellt.

setzt. Die meisten File-Sharing-Konzepte haben einen zentralen Suchserver, mit dem alle Teilnehmer verbunden sind. Der Download findet zwar per Peer-to-Peer statt, doch gesucht wird über einen zentralen Server. Fällt der Server jedoch aus, bedeutet dies gleichzeitig den Ausfall des gesamten Netzes. Bei Edonkey sind nicht nur die Dateien auf die Teilnehmer ausgelagert, sondern auch die Server. Sprich: Es gibt keinen zentralen Suchserver, mit dem alle verbunden sind. Die Anwender selbst können Suchserver einrichten. Das Edonkey-Netzwerk ist demnach völlig autark und somit immun gegen Deaktivierung eines zentralen Netzwerk-Knotens.

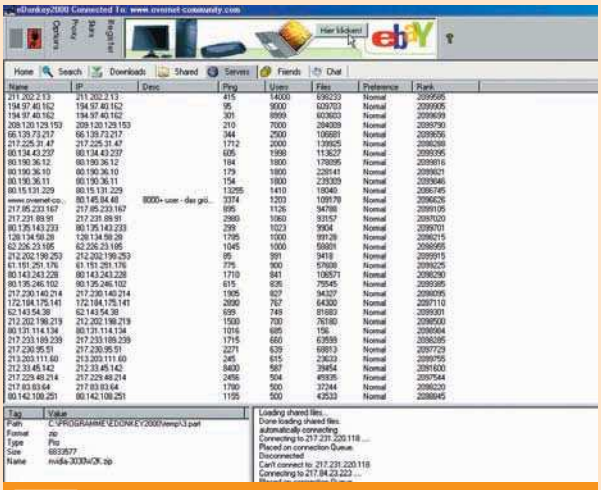
So viele Vorteile müssen auch einen „Pferdefuß“ haben: Die meisten privaten Anwender, die einen Suchserver zur Verfügung stellen, verfügen über Internet-Zugänge mit dynamischen IP-Adressen. Der daheim installierte Client kann somit nur wenige Suchserver finden. Edonkey benötigt fast täglich eine aktualisierte Serverliste. Im Web finden Sie zahlreiche Webseiten, auf denen Sie Listen mit aktuellen und aktiven Servern laden können. Die bekannteste Liste ist vermutlich ocbmaurice.dyns.net/pl/slist.pl. Mit einen Klick auf „Add all“ (Internet Explorer) werden alle aktuellen Serverdaten ins Edonkey geladen.

Eine weitere Besonderheit ist die Suchfunktion. Wenn Sie einen Suchbegriff eintippen und auf „Submit“ klicken, werden meist nur wenige Ergebnisse angezeigt. Grund: Der Client schickt den Suchbefehl erst an den Server, mit dem er selbst verbunden ist. Ihnen werden nur die Dateien gezeigt, deren Besitzer ebenfalls mit diesem Server verbunden sind. Wer seine Suche auf weitere Server ausdehnen will, muss anschließend auf die Schaltfläche „Extend Search“ klicken und die Suche wird auf den nächsten in der Serverliste stehenden Suchserver ausgedehnt; ein weiterer Klick auf den Übernächsten und so fort.

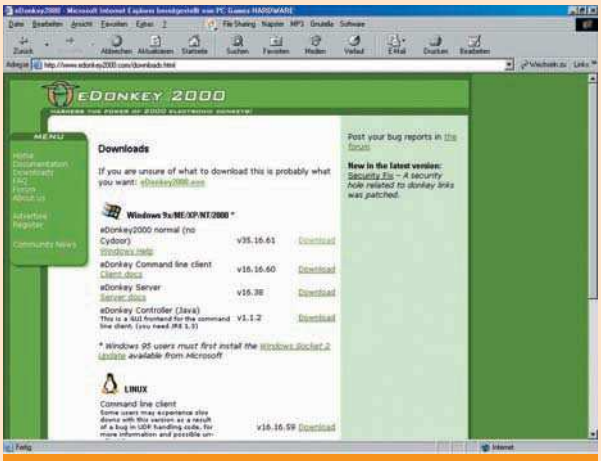
Sollten wir Ihr Interesse für Edonkey geweckt haben, dann laden Sie sich den aktuellen Client unter www.edonkey2000.com herunter. Nach der Installation müssen Sie auf jeden Fall einige Einstellungen vornehmen, damit Ihre Internetleitung nicht verstopft wird. Klicken Sie dazu auf „Options“ und setzen Sie einen Haken bei „Always stay connected“. Die Werte für „Max Upload Speed“ sollten Sie nicht auf „0“ stehen lassen. Eine Upload-Geschwindigkeit von 10 KB/s ist das Minimum, bei dem der Client noch den vollen Download-Speed zulässt. Wer weniger als 10 KB/s einstellt, dem kappt der Client auch den Download. Für T-DSL-Kunden sind 10 KB/s optimal, da so noch genügend Bandbreite für Browser und E-Mail-Programm zur Verfügung steht. Läuft der Rechner ungenutzt, können Sie den Upload auch höher setzen, allerdings sollte 14 KB/s der höchste Wert sein. Da sonst nicht nur der Upload, sondern auch der Download gebremst wird. „Max Connections:“ stellen Sie auf einen Wert von 600 bis 999. Anschließend müssen Sie sich wie weiter oben beschrieben eine aktuelle Serverliste laden. In der Registerkarte „Shared“ legen Sie fest, welche Dateien für andere Nutzer zur Verfügung stehen. Beachten Sie aber immer die Copyrights der freigegebenen Dateien. Grundsätzlich wird jedes Byte, das Sie mit Edonkey laden, gleichzeitig für andere Anwender zum Download angeboten. Demnach machen Sie sich schon mit dem Herunterladen von urheberrechtlich geschütztem Material strafbar und nicht erst durch das Anbieten!

Webseiten wie Planet3dnow.de bieten neben den herkömmlichen Serverlinks auch Verknüpfungen zu Dateien im Edonkey-Netzwerk an. Möchten Sie einen Link von einem Demo, Treiber oder Patch auf Ihren Rechner weitergeben, müssen Sie sich die Datei in der Sektion „Shared“ anzeigen lassen. Mit der rechten Maustaste klicken Sie darauf und wählen „Copy to Clipboard“. Nun können Sie den Link in eine E-Mail oder auf eine Webseite einfügen, beachten Sie bitte das Urheberrecht.

MARCO ALBERT



SERVER Damit Edonkey ordnungsgemäß funktioniert, müssen Sie häufig die Serverliste aktualisieren – am besten einmal täglich.



EDONKEY 2000 Den Client für das Edonkey-Netzwerk gibt es für Windows und Linux. Einfach laden und mit unserem Artikel konfigurieren.

Rechtsbelehrung

Können Sie der Versuchung widerstehen, einen aktuellen Filmtitel in der Suchmaske einzugeben?

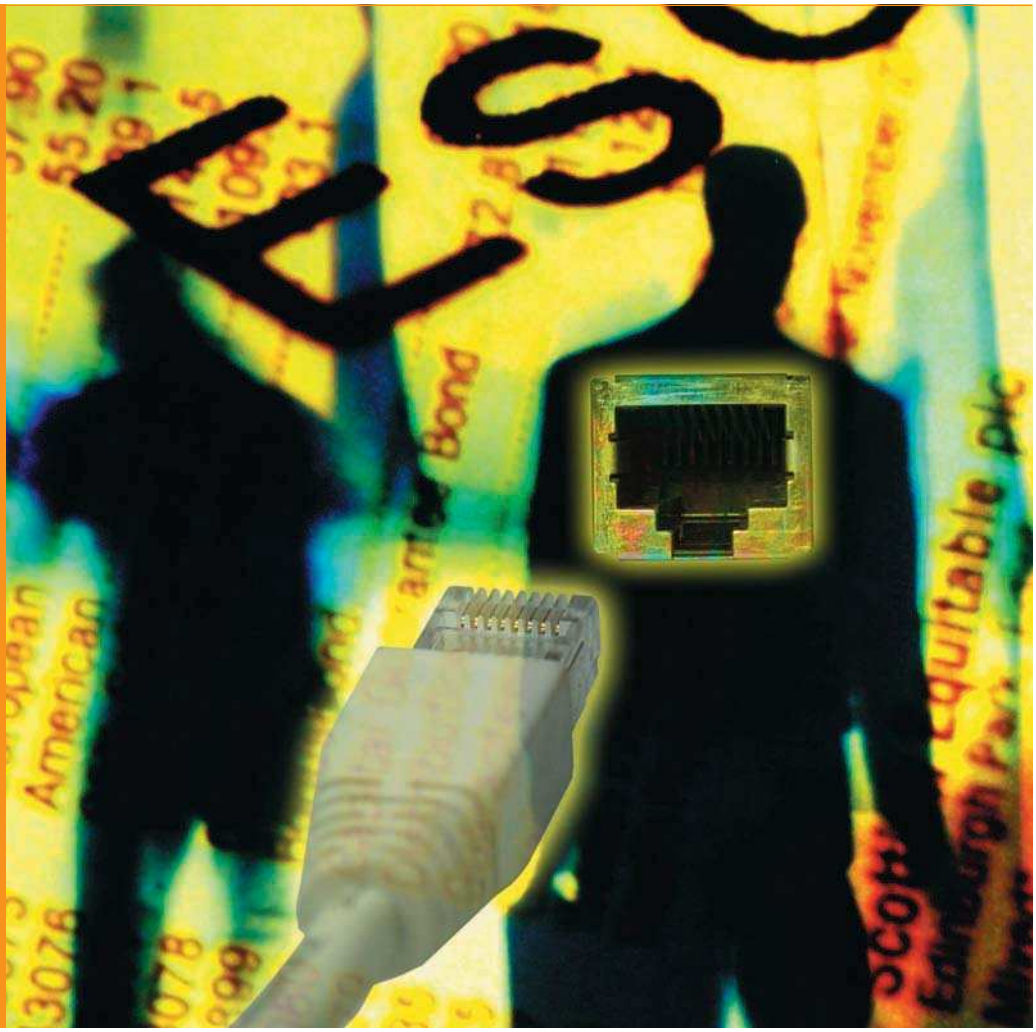
Mit dem Suchsystem von Edonkey können Sie sich auch aktuelle Treiber herunterladen.

Falls Sie mit dem Gedanken spielen, überlegen Sie sich gut, welche rechtlichen Folgen das nach sich ziehen kann. Selbst wenn Sie keine Datei zum Upload freigeben: Jene, die Sie gerade laden, steht in jedem Fall den anderen Anwendern im Netz zur Verfügung. Wer sich gerne Filme oder Musik aus dem Web saugt, sollte sich dessen bewusst sein. Sie machen sich in dem Moment strafbar, in dem Sie das erste Byte herunterladen. Grund: Sie bieten diese Files im gleichen Moment auch zum Download an, was gegen bestehende Gesetze verstößt, sofern es sich um urheberrechtlich geschütztes Material handelt. T-Online hat in diesem Zusammenhang schon Kunden abgemahnt. File-Sharing-Programme alleine brechen noch keine Gesetze, erst die Anwender tun dies.

Sicher vor 0190-Abzocke

Gib Dialern keine Chance

Wenn es um die Sicherheit Ihres PCs geht, gilt es keine Zeit zu verlieren. Deshalb haben wir für Sie diesen Sicherheits-Tuning-Dreiteiler zusammengestellt, mit dem Sie Ihren PC in null Komma nix gegen sämtliche Gefahren absichern.



TEIL 1

Im ersten Teil stehen die so genannten Dialer im Mittelpunkt. Dabei handelt es sich kleine Einwahl-Programme, die eine DFÜ-Verbindung zu einer gespeicherten Rufnummer aufbauen. Leider werden diese oft missbraucht, um teure 0190- oder 0900-Rufnummern anzuwählen. Der Nutzer bemerkt den Missbrauch meistens erst, wenn eine völlig überhöhte Telefonrechnung ins Haus flattert.

Tipp 1: Dialer erkennen

SCHWIERIGKEIT: FÜR EINSTEIGER

Ein Dialer ist in den meisten Fällen eine einzelne, ausführbare Datei, welche entweder selbst die Internetverbindung aufbaut oder einen Eintrag im DFÜ-Netzwerk erstellt und diesen anwählt. Anfangs wurden diese Einwahlprogramme zur Bezahlung von Internet-Dienstleistungen über die Telefonrechnung verwendet (die Programme waren meist auf Erotik-Websites zu finden), doch diese Zeiten sind längst vorbei. Betrüger und Abzocker haben die Chance auf das schnelle Geld gewittert. Hinter einem vermeintlichen Treiber-Update oder Gratis-Spiel kann sich ein 0190-Dialer verstecken, deshalb sollten Sie gewünschte Dateien immer von den Hersteller-Websites oder wenigstens größeren, seriösen Websites beziehen. Doch auch hier ist Vorsicht geboten, denn leider wurden in der Vergangenheit Markennamen wie Microsoft oder Winzip missbraucht, um zwielichtige Einwahlprogramme unter ahnungslosen Nutzern per Mail beziehungsweise „falschem“ Download zu verbreiten.

Dialer werden oft über einfache Downloadfenster angeboten, die Sie mit „OK“ bestätigen müssen. Das Programm wird ausgeführt, wenn die heruntergeladene Datei geöffnet wird.

WAS IST?

Dialer
Programm zur direkten Einwahl von Telefonnummern und gebührenpflichtigen Diensten

ActiveX-Control
Tool zur dynamischen Steuerung von Webseiten; kann Browser und Windows von außen aktivieren

Anti-Dialer-Tools
Programme, die in der Lage sind, Dialer auf Ihrem System aufzuspüren und zu löschen

Registry
Datenbank von Windows,die alle wichtigen Informationen über Soft- und Hardware speichert

Auch über ActiveX lässt sich leicht ein solches Einwahlprogramm auf den PC schmuggeln; so erzeugen einige Websites beim Laden eine Fehlermeldung und fordern auf, ein Plug-In zu installieren, um die Seite richtig anzeigen zu können. Ein Klick auf „Ja“ installiert statt des Plug-Ins den Dialer auf Ihrem Computer. Auch angebliche Sicherheitszertifikate, die den Betreiber seriös erscheinen lassen sollen, können einen Dialer verstecken. Nicht jeder Internetsurfer ist jedoch gefährdet: Wenn Sie die Verbindung mit dem Internet über ein Netzwerk, ein Kabelmodem oder ein ADSL-Modem herstellen, müssen Sie sich keine Sorgen machen. Die Dialer benötigen ein analoges Modem oder eine ISDN-Karte, um die gespeicherte Rufnummer wählen zu können. Auch alle AOL-Mitglieder sind geschützt. Die Software des Online-Dienstes bedient sich nicht des DFÜ-Netzwerks.

Tipp 2: PC schützen

SCHWIERIGKEIT: FÜR EINSTEIGER

Richtige Browsereinstellungen (zum Beispiel deaktiviertes ActiveX, kein automatischer Dateidownload und keine automatische Installation von Desktopobjekten) schützen vor Dialern, die sich automatisch installieren. Wer ganz sicher gehen will, kann auch Javascript deaktivieren, welches allerdings auch von vielen sicheren Websites verwendet wird. Lesen Sie jede Fehlermeldung und jedes Dialogfeld aufmerksam durch und klicken Sie im Zweifelfall immer auf „Abbrechen“ oder „Cancel“. Öffnen Sie niemals Anhänge von E-Mails, die Sie nicht angefordert haben.

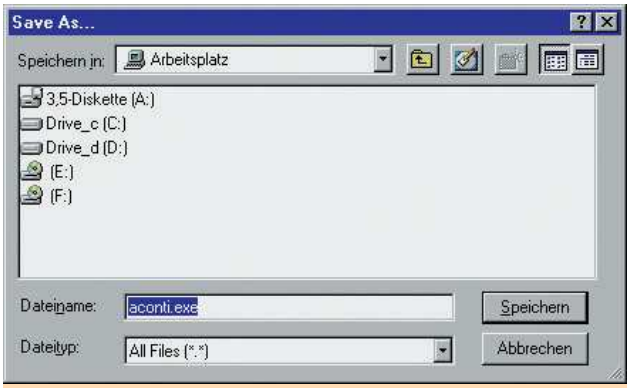
Um die Einwahl zu verhindern, verwenden Sie am besten einen der zahlreichen Dialer-Detektoren wie YAW oder 0190-Warner. Den ungewollten Zugriff auf das Internet verhindert eine Personal Firewall wie Zone Alarm oder Sygate Personal Firewall Pro. Speichern Sie Ihr DFÜ-Passwort nicht ab, so dass Sie es bei jeder Einwahl neu eingeben müssen. Gelingt eine Einwahl ohne Passworteingabe, steckt vermutlich ein Dialer dahinter, der sich als Standardverbindung eingetragen hat. Wenn Sie ein externes Modem besitzen, schalten Sie es nur dann ein, wenn Sie wirklich eine Verbindung ins Internet erstellen wollen. Nach getrennter Verbindung schalten Sie das Modem wieder aus, so kann sich kein Dialer in Ihrer Abwesenheit einwählen. Wenn Sie sicher sind, dass Sie keine Mehrwert-Dienste mit den einschlägigen Vorwahlen in Anspruch nehmen wollen, können Sie diese auch von der Telefongesellschaft sperren lassen. Empfehlenswert ist die Sperre der folgenden Vorwahlen: 0190, 0192, 0193 und 0900.

Tipp 3: Dialer entfernen

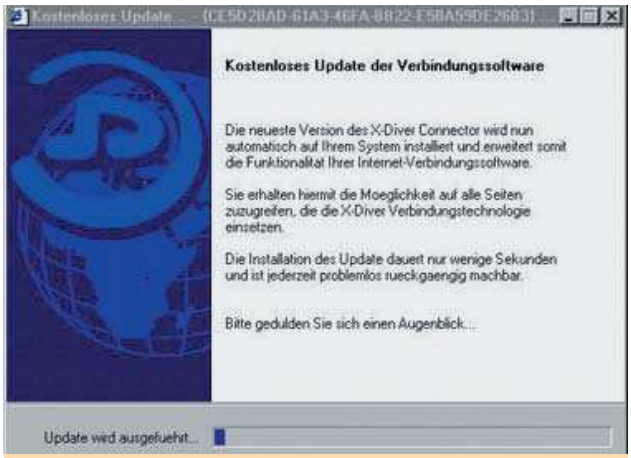
SCHWIERIGKEIT: FÜR EINSTEIGER

Ein Dialer ist kein Virus und kann deshalb auch von keinem Anti-Virus-Programm ohne spezielle Dialer-Erkennung unschädlich gemacht werden. Sie müssen sich also zunächst manuell auf die Suche machen. Sehen Sie im DFÜ-Netzwerk nach, ob eine weitere Verbindung erstellt wurde; ist eine vorhanden, löschen Sie diese. Stellen Sie die Standardverbindung im Browser auf Ihren Provider um, falls diese vom Dialer verstellt wurde.

Öffnen Sie den Task-Manager mit der Tastenkombination „Strg“, „Alt“ und „Entf“ und durchsuchen Sie die Liste der geöffneten Tasks nach ungewöhnlichen Einträgen. Wenn der Dialer zum Beispiel „dialer.exe“ heißt, verwenden Sie die Windows-Suchfunktion unter „Start“ – „Suchen“ – „Nach Dateien oder Ordnern“ und suchen Sie nach der Datei, in unserem Fall „dialer.exe“. Löschen Sie die Datei, wenn Sie sich absolut sicher sind, dass es sich hierbei um einen Dialer handelt. Sehen Sie nach, ob sich im Autostart-Ordner eine Verknüpfung zum Dialer befindet. Finden Sie ihn nicht im Autostart-Ordner, wird er wahrscheinlich über die Registry oder die Systemdateien gestartet. Die Registry durchsuchen Sie mit dem Tool „Regedit“, welches Sie im Windows-Ordner finden, die Systemdateien können mit „Sysedit“ komfortabel bearbeitet werden (ebenfalls im Windows-Ordner).



1 **DOWNLOAD** Es ist ratsam, keine Files herunterzuladen, wenn Sie deren Herkunft nicht kennen oder sie dubiose Internetseiten anbieten.

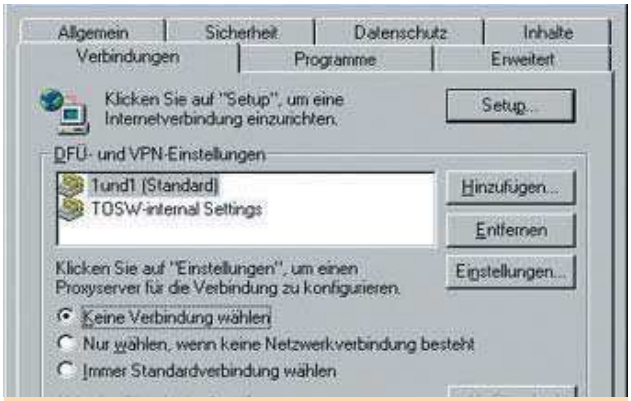


1 **FALSCHE ANGABEN** Oftmals wird der Nutzer durch falsche Versprechen dazu „überredet“, die Installation zuzulassen.

1 **ZERTIFIZIERT** Falsche Zertifikate werden benutzt, um dem Nutzer Seriosität und Vertrauenswürdigkeit vorzugaukeln.

2 **ENTTARNT** Entdecken Sie nach einem Internet-Besuch plötzlich ein unbekanntes Symbol auf der Taskleiste, könnte es ein Dialer sein.

3 DFÜ-VERBINDUNGEN Die zweite Verbindung, die Sie hier sehen, wurde von dem Dialer automatisch erstellt.



3 DIALER-ÄNDERUNGEN Ohne dass Sie es bemerken, nimmt der Dialer selbstständig Änderungen an Ihrer Standardverbindung vor.

3 WINDOWS-REGISTRIERUNG Wissen Sie, dass Sie sich einen Dialer eingefangen haben, sollten Sie in der Registry nach ihm suchen.

4 KOSTENFALLE Das Bild soll hier wohl vom Kleingedruckten ablenken: Dieser Dialer kostet sage und schreibe 900 Euro pro Einwahl!

5 AKTIVSCHUTZ Dialerschutzprogramme wie YAW scannen Laufwerke auf Dialer-Einträge und isolieren oder löschen diese Einträge.

Die verbliebenen Einträge können Sie mit Microsofts Regclean entfernen. Wenn der gelöschte Dialer beim nächsten Systemstart wieder erscheint, kann dies an der Datei „winsvc32.exe“ oder „openme.exe“ liegen. Löschen Sie diese und sämtliche Schlüssel in der Registry, die deren Namen enthalten. Leeren Sie vorsichtshalber auch den Cache Ihres Browsers und den Temp-Ordner. Wir möchten an dieser Stelle darauf hinweisen, dass das Modifizieren der Registry dazu führen kann, dass Windows nicht mehr richtig startet und eine Neuinstallation des Betriebssystems erforderlich ist.

Tipp 4: Recht einklagen

SCHWIERIGKEIT: FÜR EINSTEIGER

Haben Sie einen Dialer installiert, um beispielsweise eine Erotik-Webseite zu betrachten, können Sie nichts gegen den Anbieter unternehmen. Sie haben eine Leistung in Anspruch genommen und müssen diese bezahlen. Die Strafverfolgungsbehörden prüfen Ihre Angaben sehr genau, falsche Aussagen können Ihnen eine Anzeige wegen Vortäuschung einer Straftat einbringen. Um Sie als Verbraucher besser vor der 0190-Abzocke zu schützen, hat der Wirtschaftsausschuss im Bundesrat die Telekommunikations-Kundenschutzverordnung verabschiedet. Die Telefon-Netzbetreiber müssen nun Auskunft über einen Anbieter, der Forderungen auf einer Rechnung erhebt, erteilen. Falls Sie also einen 0190-Dialer auf Ihrer Telefonrechnung finden, den Sie oder andere Nutzer des betroffenen Systems nicht installiert haben, sollten Sie rechtliche Schritte in Erwägung ziehen.

Tipp 5: Treffen Sie Vorsichtsmaßnahmen!

SCHWIERIGKEIT: FÜR FORTGESCHRITTENE

Installieren Sie am besten eines der gängigen Anti-Dialer-Tools wie „YAW“ (Yet Another Warner, www.yaw.at) oder „0190-Warner“. Informationen zum Thema Dialer und Abwehr finden Sie im Internet vor allem unter der Adresse von „Dialerschutz.de“ (www.dialerschutz.de). Dort gibt es nicht nur sehr viele Informationen zu Dialern und deren Funktionen oder Auswirkungen, sondern auch viele Tools gegen Dialer sowie Hilfestellungen für den Fall, dass ein Dialer zugeschlagen hat. Wenn Sie im Web surfen und Seiten mit nicht regulären Inhalten besuchen, müssen Sie sich der Gefahr bewusst sein, dass solche Inhalte oft nur durch gebührenpflichtige Wählprogramme genutzt werden können. Sofern Sie gesondert auf das Angebot, die Gebühren sowie den zustande kommenden Vertrag hingewiesen werden, handelt es sich in der Regel um ein seriöses Angebot. Finden Sie jedoch plötzlich Download-Anfragen oder ein Programm versucht automatisch, ein „Plug-In“ für Ihren Browser zu aktivieren, sollten Sie die Verbindung sofort abbrechen und die Seite verlassen. Sind Sie nicht sicher, ob ein Dialer tatsächlich installiert wurde, installieren Sie eines der Dialerschutz-Tools und scannen Sie Ihre Datenträger auf verdächtige Eintragungen. Inspizieren Sie auch den DFÜ-Netzwerkeintrag auf sichtbare Änderungen der Einwahl (lesen Sie hierzu „Schluss mit der Abzocke“ in diesem Heft).

JIVKO SEIZOV/FRANK MISCHKOWSKI/
CHRISTIAN GÖGELEIN

USB Link Kabel

USB Card Reader

USB Infrarot Adapter

USB Aktiv Verlängerung

USB 2.0/1.1/Firewire
PCMCIA Karten

USB 2.0/1.1/Firewire
PCI Karten

USB Smart Hub Pro

Interne USB &
Firewire Hubs

USB Share AutoSwitch

USB Smart Hub

KVM Switch USB
(Monitor-, Maus & Tastatur-Umschalter)

USB 2.0/1.1/Firewire
Laufwerksgehäuse
(Festplatte, CD, DVD, Writer, ...)

LINDY®
COMPUTER CONNECTION TECHNOLOGY

Im gut sortierten Fachhandel!

Ihren Fachhändler
erfahren Sie unter:
Tel: 0621.47005-0

neu-besser-schneller-**www.lindy.de**

LINDY, Ihr Spezialist für:

- USB und Firewire Produkte
- KVM Switches (Monitor-, Maus & Tastatur-Umschalter)
- Computerkabel
- PC Steckkarten & PCMCIA
- Netzwerkprodukte
- Computer Connectivity

LINDY auf der CeBIT Halle 15 Stand A 28

CeBIT
HANNOVER
12. – 19. 3. 2003

LINDY-Elektronik GmbH
Markircher Str. 20
D-68229 Mannheim

Tel 0621.47005-0
Fax 0621.47005-30
E-Mail: info@lindy.de

Anonym und sicher durchs Netz

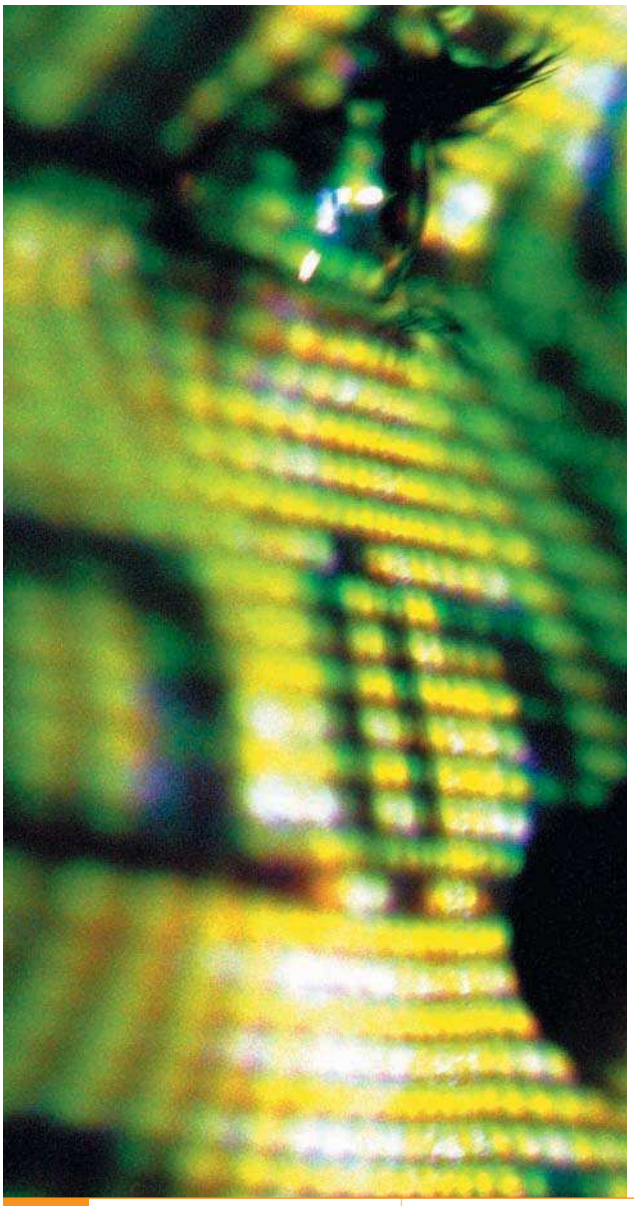
Schützen Sie Ihre Identität

ARBEITSMATERIAL
- Adaware
- Internet Explorer
- Proxy-Server

ZEITAUFWAND
30 Minuten

TEIL 2

Gefahren aus dem Netz können Ihnen nicht nur finanziellen, sondern auch persönlichen Schaden zufügen: Hacker, Spyware, Trojaner untergraben Ihre Privatsphäre. Wir zeigen, wie Sie sich schützen.



Nahezu jede Website, auf die Sie surfen, speichert Ihre Daten, um den Benutzer bei einem späteren Besuch wiedererkennen zu können. Einige Programme übermitteln sogar Daten an den Website-Betreiber. Wir zeigen, wie Sie solche Seiten beziehungsweise Programme erkennen und die Datenübermittlung unterbinden können.

Tipp 1: Cookies regelmäßig löschen

SCHWIERIGKEIT: FÜR EINSTEIGER

Cookies sind kleine, maximal vier Kilobyte große Textdateien, welche vom Browser angelegt werden. Cookies sind ungefährlich, sie sind nicht ausführbar und können somit keine Viren oder Programme enthalten. Die Aufgabe eines Cookies ist die Zwischenspeicherung von Informationen, die das Surfen und die Kommunikation mit dem Webserver vereinfachen soll. Anwendungsbereiche sind beispielsweise Warenkörbe in Online-Shops oder persönlich zugeschnittene Websites. Auch die Speicherung von Benutzerkennungen – zum Beispiel für Diskussionsforen, damit Sie sich nicht bei jedem Besuch neu einloggen müssen – wird durch Cookies realisiert.

Durch die Speicherung Ihrer Benutzerkennung können Anbieter allerdings Ihr Surfverhalten analysieren und ein Nutzerprofil erstellen. Eine weitere Gefahr der Cookies ist, dass unbefugte Personen an Ihrem Rechner Daten einsehen könnten, wenn Sie sich beispielsweise auf einer Website per Cookie automatisch einloggen. Meistens geben die Anbieter den Cookies ein „Verfallsdatum“ mit, nach Ablauf werden diese von der Festplatte gelöscht. Um den Ordner, in dem die Cookies abgelegt werden, zu finden, benutzen Sie die Windows-Suche und suchen Sie nach dem Ordner „Cookies“. Auf einem Standard-Windows-2000-System mit dem Internet Explorer 6 lautet der Pfad „C:\Dokumente und Einstellungen\Benutzername\Cookies“. Hier finden Sie zahlreiche Textdateien, die in der Form Benutzername@Server.txt abgelegt wurden. Im Browser selbst können Sie unter „Allgemein“ auch gleich alle Cookies auf einmal löschen.

Tipp 2: Java und ActiveX

SCHWIERIGKEIT: FÜR EINSTEIGER

Java ist eine von Sun entwickelte Programmiersprache. Es wird zwischen Java-Programmen, Java-Applets und Java Script unterschieden. Java-Programme sind unabhängig vom Betriebssystem und laufen nur im Web-Browser. Javascript ist eine rei-

WAS IST?

Spyware
Software, die den Nutzer ausspioniert und persönliche Daten an den Hersteller übermittelt

Javascript
Häufig eingesetzte Programmiersprache, die den HTML-Befehlssatz erweitert

ActiveX
Programmierschnittstelle für Web-Anwendungen. Als Microsoft-Alternative zu Java geplant.

Sandbox
Sichere Browser-Umgebung, in der ausschließlich Java-Codes ausgeführt werden

Schutzwall für jedermann

Unter www.zonelabs.com gibt es die sehr gute Firewall Zone Alarm zum kostenlosen Download.

Zone Alarm meldet sofort, wenn jemand von außen versucht, Ihren PC anzugreifen.

Zone Alarm in der kostenlosen Variante bietet zwar weniger Funktionen als die Pro-Version, für den Privatgebrauch reicht der Schutz aber allemal.

ne Scriptsprache, die ursprünglich von Netscape auf Basis von Java entwickelt wurde und als Erweiterung des HTML-Codes dient. Gefahr geht vor allem von Java-Applets aus: Diese sind allerdings nur in einem Java-fähigen Browser lauffähig. Der Microsoft Internet Explorer verwendet hierfür die so genannte Virtual Machine. Die Gefahren durch Java sind relativ gering, da Java-Applets nur in der „Sandbox" laufen, die Risiken liegen lediglich in Programmierfehlern, die den Browser zum Abstürzen bringen können. Abhilfe schafft das Deaktivieren von Java, das aber von vielen Webseiten mit Fehlermeldungen quittiert wird.

Tipp 3: ActiveX besser abschalten

SCHWIERIGKEIT: FÜR EINSTEIGER

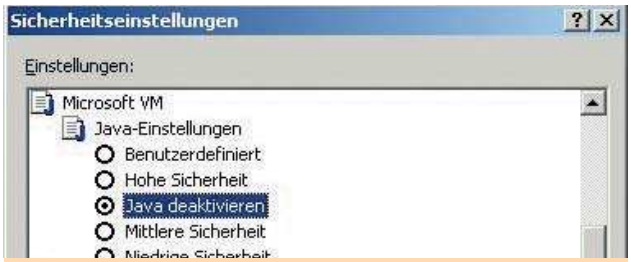
ActiveX ist eine von Microsoft entwickelte Programmierschnittstelle für Web-Anwendungen. Bei der Konzeption wurde komplett auf Sicherheitseinschränkungen, wie sie Java besitzt, verzichtet. ActiveX-Elemente können wie Windows-DLL-Dateien unter anderem Betriebssystemfunktionen aufrufen (zum Beispiel den PC herunterfahren beziehungsweise neu starten) oder sogar auf das Dateisystem zugreifen (Daten lesen, schreiben, umbenennen beziehungsweise löschen). Die Gefahren sind unüberschaubar, daher sollten Sie ActiveX unbedingt deaktivieren. Im Microsoft Internet Explorer tun Sie dies über die verschiedenen Sicherheitsstufen. Um sicher zu gehen, sollten Sie sämtliche ActiveX-Funktionen deaktivieren. Ein guter Kompromiss zwischen Sicherheit und Kompatibilität ist die Stufe „Mittel". Verwenden Sie einen anderen Browser wie Opera, Netscape oder gar ein alternatives Betriebssystem wie Linux, sind Sie auf der sicheren Seite, denn hier lässt sich Microsofts Antwort auf Java gar nicht erst verwenden.

Tipp 4: Spyware wieder loswerden

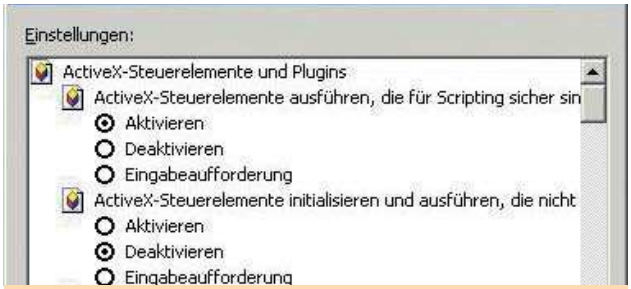
SCHWIERIGKEIT: FÜR EINSTEIGER

Als Spyware werden Programme bezeichnet, die Informationen sammeln und an den Hersteller weiterleiten. Sie ist mit der so genannten Adware nahe verwandt. Zur Adware zählen Programme, die durch das Einblenden von Werbebannern finanziert werden. Diese laden sich nicht nur Werbebanner aus dem Internet, sondern senden auch oftmals das mitprotokollierte Surfverhalten des Nutzers an den Softwareanbieter. Der Nutzer des Programms merkt von der Übertragung nichts. Auch einige prominente Programme lassen sich in die Kategorie „Spyware" einordnen. Bekannte Beispiele wären der Babylon Translator, der E-Mail-Client Eudora oder das Fileshare-Tool Kazaa. Dies gilt aber nur für die werbefinanzierten Versionen mit Bannern, die registrierten Vollversionen übertragen keine Daten. Zur Erkennung und Beseitigung von Spyware empfehlen wir das Tool Adaware von Lavasoft. In der aktuellen Version 5.83 werden

1 INTERNET-OPTIONEN Bei den Internet-Optionen in der Systemsteuerung können die Cookies gelöscht werden.

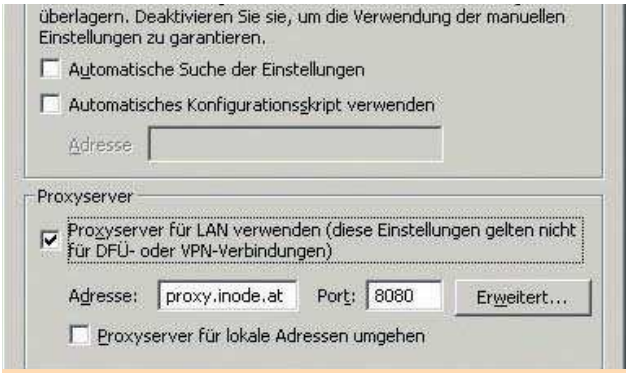


2 SICHERHEITSEINSTELLUNGEN Auch Java sollten Sie trotz Virtual-Machine-Umgebung in den Sicherheitseinstellungen deaktivieren.

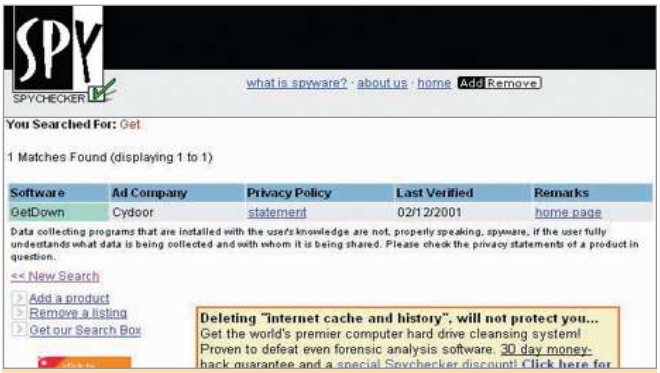


3 SICHERHEITSEINSTELLUNGEN ActiveX stellt ein besonders hohes Sicherheitsrisiko dar und sollte abgeschaltet werden.

4 ADAWARE Das Sicherheits-Tool Adaware spürt Spyware in Registry, Cookies sowie Laufwerken auf und eliminiert sie.

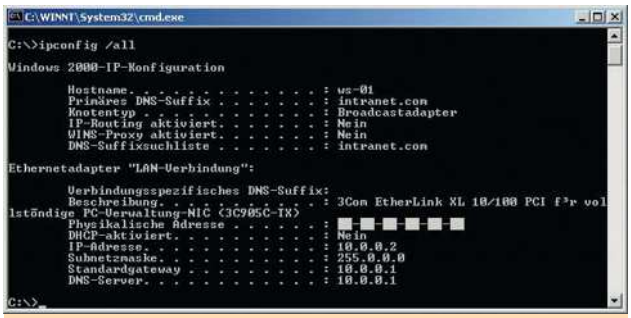


5 INTERNET-OPTIONEN In den Browser-Einstellungen wird unter anderem die IP-Adresse des Proxy-Servers eingetragen.



5 ONLINE-PRÜFER Auf www.spychecker.com können Sie online überprüfen, ob eine Software Spyware enthält, und es gibt Tipps, diese zu entfernen.

5 WHATISMYIP.COM Von Anonymität keine Spur: Webseiten können leicht Ihre IP-Adresse auslesen und speichern.



5 IPCONFIG Ipconfig zeigt unter Windows NT, 2000 und XP die zugewiesene IP-Adresse des Rechners an.

6 METACRAWLER Die Suchmaschine Metacrwaler.de bietet einen Proxyserver an, mit dem man gefundene Seiten anonym öffnen kann.

Arbeitsspeicher, Cookies, Registry und Programme überprüft, anschließend entscheiden Sie, ob die Spyware unschädlich gemacht werden soll. Für den Fall, dass das Programm nach der Säuberung nicht mehr läuft, legt Adaware ein Backup der veränderten Dateien an, so dass kein Schaden an Ihren Daten entsteht. Ist man nicht sicher, ob eine Shareware-Version mit Spion-Software verseucht ist, lohnt sich ein Besuch auf der Website des „Spy-Checker“ (www.spychecker.com). Hier können Sie einen Online-Check vornehmen, indem Sie den Namen einer Software in eine Datenbanksuche eingeben. Eine weitere Möglichkeit zur Verhinderung der Datenübertragung ist eine Personal Firewall wie Zone Alarm. Hier können Sie Programmen den Zugriff auf das Internet verbieten, so dass keine Daten mehr an den Hersteller übermittelt werden.

Tipp 5: Anonym und sicher surfen

SCHWIERIGKEIT: FÜR EINSTEIGER

In letzter Zeit gibt es gute Gründe, seine Anonymität im Internet zu wahren. Diskussionsforen speichern Ihre Aussagen länger als das Gedächtnis, Sie können Jahre später damit konfrontiert werden. Einige Unternehmen lassen sogar schon Online-Profile von ihren Bewerbern anfertigen. Nahezu jedes Diskussionsforum speichert neben den Beiträgen auch die IP-Adresse. Je nach Internet-Provider bekommen Sie eine statische (selten) oder eine dynamische IP-Adresse (meistens), wobei die dynamische IP eine spätere Identifikation des Surfers erschwert. Sie finden Ihre eigene IP-Adresse unter Windows 9x heraus, indem Sie unter „Start“ – „Ausführen“ den Befehl „Winipcfg“ eingeben. Benutzer von Windows NT, 2000 oder XP müssen hierfür „Ipconfig-all“ eingeben. Alternativ zeigt Ihnen auch die Website www.whatismyip.com Ihre IP-Adresse an.

Tipp 6: IP-Adresse mit Proxy verschleiern

SCHWIERIGKEIT: FÜR EINSTEIGER

Die IP-Adresse lässt sich durch die Verwendung eines Proxy-Servers verschleiern. Ein Proxy-Server ist ein Rechner im Internet, der anstelle Ihres Rechners Webseiten abruft und sie an Ihren PC weiterleitet. Statt der eigenen IP-Adresse wird die des Proxys an den Webserver gesandt. Sie können aber auch einen speziellen, anonymen Proxy-Server verwenden. Der Unterschied zwischen normalen und anonymen Servern ist, dass letztere keine Log-Files anlegen und sich somit der Benutzer nicht zurückverfolgen lässt. Vergleichen Sie die IP-Anzeige von Winipcfg mit der von Whatismyip.com. Wenn sich die IP-Adressen unterscheiden, surfen Sie über den Proxy-Server.

JIVKO SEIZOV/CHRISTIAN GÖGELEIN/FRANK MISCHKOWSKI

Webseiten

http://home.t-online.de/home/TschiTschi/java_activex.htm – ActiveX und Javascript
http://www.lavasoftusa.com – Lavasoft Ad-Aware
http://www.computec.ch/dokumente/firewalling/anonyme_proxies – Anonyme Proxies

Viren, Würmer und Trojaner

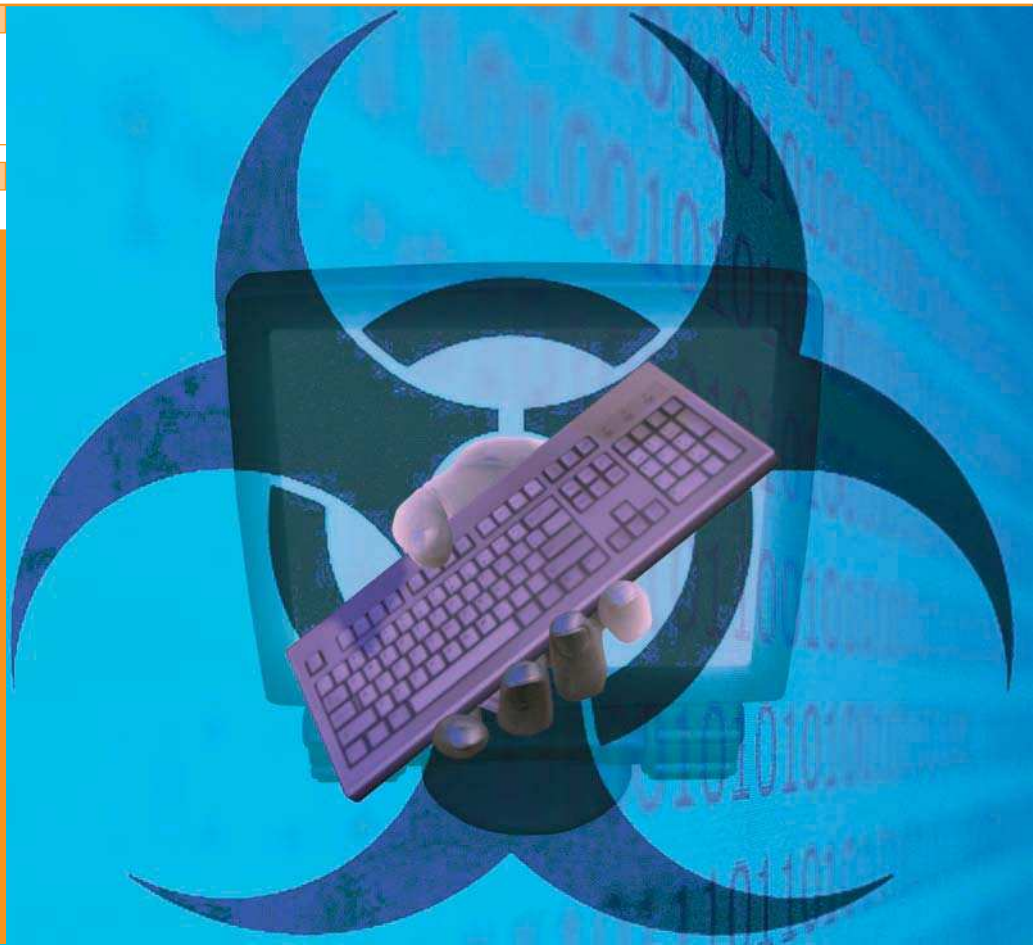
Gefahren aus dem Netz

ARBEITSMATERIAL

- Norton Antivirus 2003
- Zone Alarm 3.1.395
- H+B Antvir

ZEITAUFWAND

30 Minuten



TEIL 3

Viren und Trojanische Pferde stehen für Datenraub und -zerstörung. Haben Sie sich vielleicht bereits infiziert? Hätte es verhindert werden können?

Im dritten Teil unserer Sicherheits-Serie zeigen wir Ihnen, wie Sie Viren und Trojaner erkennen und Ihren PC davor schützen.

Tipp 1: Alarmstufe Rot: Viren an Board

SCHWIERIGKEIT: FÜR EINSTEIGER

Wenn ein PC mit einem Virus infiziert wird, kann der Schaden stark variieren. So begnügen sich harmlosere Schädlingsvarianten damit, den Nutzer mit Dialogboxen und dem Abspielen von Sounds zu penetrieren. Hinterhältigere Zeitgenossen benennen Dateien um und sorgen so für große Verwirrung. Die Bezeichnung Virus steht also für eine ganze Gruppe von virtuellen Schädlingen, die in einzelne Kategorien eingeteilt werden können.

Der Bootvirus kopiert sich beispielsweise in den Bootsektor der Festplatte oder einer Diskette und wird bei jedem Start des Rechners geladen. Einige Vertreter dieser Art verhindern so das Starten des Betriebssystems. Der Makrovirus versteckt sich hingegen in einem Office-Dokument. Auch er kann dem System großen Schaden durch das Löschen von Dateien zufügen. Der so genannte Wurm versendet sich selbst per E-Mail an sämtliche Kontakte im Outlook-Adressbuch und sorgt so für eine starke Verbreitung. Der Trojaner hingegen ist kein Virus, obwohl er oft mit diesen in einen Topf geworfen wird. Wir behandeln dieses Thema im nächsten Schritt gesondert.

Schädliche Programme können in nahezu jeder Programmier- oder Scriptsprache geschrieben werden. Sie können auch selbsttätig, ohne Anklicken der infizierten Datei, aktiv werden, da

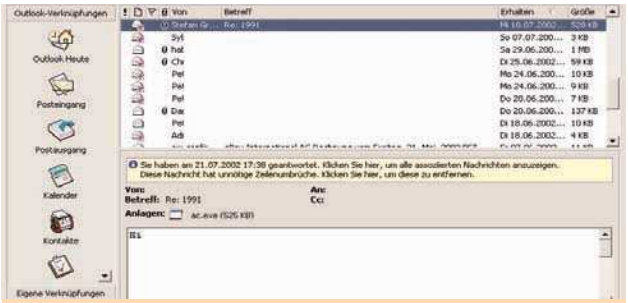
WAS IST?

Virus
Programmcode, der geschaffen wurde, um auf Computern Schaden anzurichten.

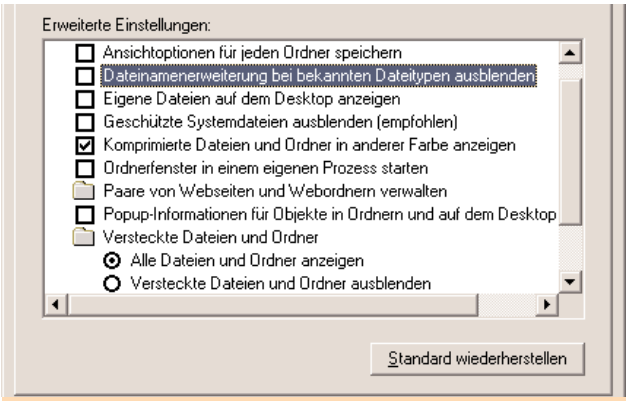
Trojaner
Befallen fremde Rechner, um diese auszuspionieren und die gesammelten Daten zu versenden.

Firewall
Software- oder Hardware-Lösung, die bestimmte Ports des PCs schließt.

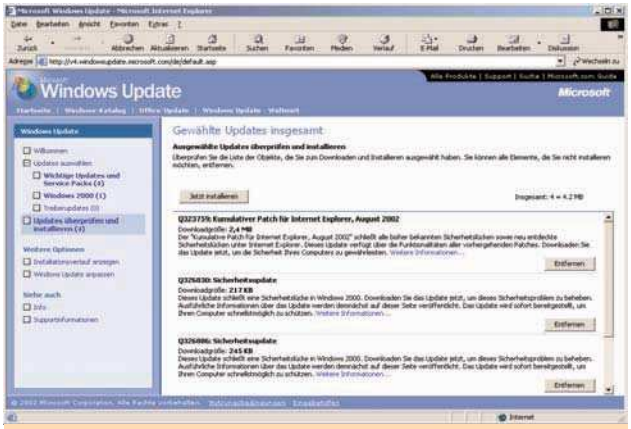
Port
Kommunikationskanal bei der Datenübertragung via TCP/IP und anderen Diensten.



1 MICROSOFT OUTLOOK Eine der „beliebtesten" Arten, Viren zu verbreiten, ist die E-Mail. E-Mail-Clients sind daher eine Gefahrenquelle.



1 ORDNEROPTIONEN Lassen Sie sich die Dateierweiterung einblenden. So wissen Sie, womit Sie es wirklich zu tun haben.



3 WINDOWSUPDATE Installieren Sie alle Sicherheits-Updates für Ihr Betriebssystem. Viele Lücken werden dadurch bereits geschlossen.

3 NORTON ANTIVIRUS Lassen Sie Ihr System regelmäßig von einem Virenscanner überprüfen. Vorsicht ist gut, Kontrolle ist besser.

sie von Windows selbst ausgeführt werden. Eine virenverseuchte Datei kann andere Dateien auf dem Rechner infizieren oder gar zerstören, selbst wenn diese einen komplett unterschiedlichen Dateityp hat. So kann zum Beispiel ein Wurm (Visual Basic Script) sämtliche MP3-Dateien auf der Festplatte zerstören.

Einer der bekanntesten Schädlinge ist der Wurm „Iloveyou", der durch seine extrem schnelle Verbreitung viele Mailserver überlastet und für mehrere Tage lahm gelegt hat. Auch die Klez-Würmer gelangten zu zweifelhaftem Ruhm. Offensichtlich wollte der Programmierer sich selbst in Szene setzen, denn der von Klez-Varianten angerichtete Schaden hielt sich im Gegensatz zur Verbreitung in Grenzen.

Tipp 2: Wie arbeiten Trojaner?

SCHWIERIGKEIT: FÜR EINSTEIGER

Die Arbeitsweise der bekannten Trojaner wie Subseven, Netbus oder Back Orifice ist immer gleich. Das Programm dient als eine Art hinterhältige Fernbedienung für den PC des Opfers – in etwa vergleichbar mit dem professionellen PC Anywhere, das Systemoperatoren zur Steuerung von externen Computersystemen wie Servern dient. Der Trojaner besteht aus zwei Teilen, dem Client, über den der Angreifer den Computer des Opfers steuert, und dem Server, der auf dem Zielrechner installiert wird. Der Schädling steht als eine Art Baukasten im Internet zum Download bereit, der Server wird über das mitgelieferte Programm so angepasst, dass er dem Angreifer die IP-Adresse des Opfers mitteilt, sobald es online ist. Über das Konfigurationsprogramm des Trojaners lässt sich beispielsweise der Server in eine eigenständige EXE-Datei packen, die nach dem Öffnen wieder verschwindet. Führt der ahnungslose PC-Nutzer dieses File aus, trägt sich der Trojaner in die Registry ein, so dass er zusammen mit Windows gestartet wird. Der Quellcode kann allerdings auch an eine andere EXE-Datei angehängt werden, wodurch dieser somit perfekt getarnt wird.

Wenn Sie nun online gehen, hat der Angreifer den vollen Zugriff auf Ihre Daten, kann jeden Tastendruck mitloggen, Programme öffnen und schließen und Sie beim Arbeiten beobachten. Einen laufenden Trojaner-Server erkennen Sie an einem unbekannten Prozess im Task-Manager oder ständiger Internet-Aktivität, obwohl Sie sämtliche Internet-Programme wie Outlook und Internet Explorer geschlossen haben. Stellen Sie diese Symptome fest, sollten Sie den Rechner schnellstens vom Internet trennen und eine entsprechende Überprüfung – wie im nächsten Schritt beschrieben – durchführen.

Tipp 3: Rechner optimal absichern

SCHWIERIGKEIT: FÜR EINSTEIGER

Die anfälligste Schnittstelle für Viren und Trojaner ist der E-Mail-Verkehr. Unter falschem Absender wurden in letzter Zeit oft Viren als Sicherheits- oder Treiber-Update getarnt. Löschen Sie solche Nachrichten sofort! Kein Hard- oder Softwarehersteller verschickt unaufgefordert Dateien. Doch auch als Gewinnspiele oder gar Liebesbriefe getarnte Viren gelangten über diesen Weg schon in Umlauf. Es gilt die Grundregel: Öffnen Sie keine Post von unbekannten Absendern, die Anhänge enthält. E-Mails im HTML-Format sind nicht nur groß und somit unhöflich 56-k-Usern gegenüber, sie bergen auch ein Risiko. Durch den HTML-Code können beispielsweise – bei entsprechend niedriger Sicherheit – unsignierte ActiveX-Elemente geladen werden, die einen Dialer enthalten. Gehen Sie auf Nummer Sicher und deaktivieren Sie ActiveX. Zudem sollten Sie auf HTML-Mails verzichten und auf das Nachrichtenformat „Nur Text" umstellen.

Ein weiterer, wichtiger Tipp: Entfernen Sie im Arbeitsplatz unter „Extras" – „Ordneroptionen" – „Ansicht" das Häkchen bei „Dateinamenerweiterungen bei bekannten Dateien ausblenden". Viren haben oft einen doppelten Dateinamen, so dass sie harmlos aussehen, wenn die richtige Dateiendung ausgeblendet ist. Eine Datei namens

„Virus.TXT.EXE“ zeigt Windows in der Standardeinstellung als „Virus.TXT“ an. Beim Versuch, die vermeintliche Textdatei zu öffnen, installieren Sie den Virus.

Grundsätzlich sollten Sie Ihre Software immer auf dem neuesten Stand halten. Prüfen Sie regelmäßig auf windowsupdate.microsoft.com, ob Updates für Ihr Betriebssystem vorhanden sind, und halten Sie auch Ihren Browser und E-Mail-Client stets auf dem Laufenden. Viele Virenscanner können sich automatisch die neuesten Virendefinitionen aus dem Internet herunterladen, verwenden Sie dieses automatische Update regelmäßig. Bei der Wahl Ihres Virenprogramms sollten Sie zudem darauf achten, dass E-Mails und Office-Dateien ebenfalls auf schädliche Programmcodes geprüft werden.

Tipp 4: Computer online prüfen

SCHWIERIGKEIT: FÜR EINSTEIGER

Um ein Sicherheitsloch zu stopfen, müssen Sie erst einmal wissen, wo sich dieses überhaupt befindet. Sie müssen allerdings keinen Hackerangriff auf Ihren Rechner starten, um sich über Schwachstellen zu informieren. Sicherheitsexperte Symantec, Hersteller von Norton Antivirus, bietet auf seiner Webseite unter www.symantec.com/securitycheck einen einfachen Online-Check an. Der Sicherheitscheck prüft Ihren Rechner unter anderem auf die Netzwerksicherheit (anonyme Zugriffe), installierte Trojaner und sonstige Sicherheitsrisiken und gibt Ihnen anschließend nützliche Tipps, wie Sie Ihre eventuell vorhandenen Sicherheitslöcher schließen können.

Neben dem Sicherheitscheck bietet Symantec auch einen Online-Virencheck an, der auf die riesige Virendatenbank von Norton Antivirus zurückgreift. Es handelt sich hierbei um eine knapp 1,5 Megabyte große Active-X-Anwendung. Sobald diese geladen ist, werden die Festplatten Ihres Rechners gescannt. Anschließend wird Ihnen das Ergebnis im Browserfenster präsentiert. Die Vorteile dieser Onlinechecks liegen auf der Hand: Die Virendefinitionen sind stets auf dem neuesten Stand, der Check erfordert keine Zusatzsoftware und kostet nichts. Jeder PC, der über einen Internetzugang verfügt, lässt sich schnell und einfach überprüfen. Einziger Wermutstropfen: Mit dieser Methode können Viren und Sicherheitslöcher nur erkannt, aber nicht beseitigt werden.

Tipp 5: Machen Sie den Viren den Garaus!

SCHWIERIGKEIT: FÜR EINSTEIGER

Sie haben Ihren PC überprüft und der Virenscanner hat herausgefunden, dass eine oder mehrere Dateien mit einem Virus infiziert sind – doch wie werden Sie die Schädlinge wieder los? Wenn die Dateien eher unwichtig sind, können Sie eine „manuelle“ Beseitigung ausprobieren, indem Sie die schädlichen Files im Datei-Manager einfach löschen. Ist allerdings kein Zugriff unter Windows möglich, gibt es die Möglichkeit, das Betriebssystem unter DOS zu rebooten. Führen Sie anschließend einen erneuten Virencheck durch. Werden die Schädlinge dann aber noch immer gemeldet, benötigen Sie einen guten Virenscanner. In den meisten Fällen können die Dateien zum Glück noch repariert werden, andernfalls werden sie entweder isoliert, so dass kein Zugriff mehr darauf erfolgen kann, oder sicher gelöscht.

Einen Trojaner stoppen Sie am besten über eine Personal Firewall wie Zone Alarm. Sobald das Trojanische Pferd eine Verbindung mit dem Internet aufzubauen versucht, erhalten Sie eine Dialogbox, in der Sie den Zugriff entweder erlauben oder verbieten können. Verbieten Sie dem Trojaner die Internetaktivität, kann er in den meisten Fällen keinen Schaden mehr anrichten. Zum Entfernen des ungebetenen Gasts finden Sie einige Tools auf www.trojaner-info.de. Alternativ sollte auch jeder gute Virenscanner in der Lage sein, Trojanische Pferde zu isolieren beziehungsweise gänzlich aus dem System zu entfernen.

JIVKO SEIZOV/FRANK MISCHKOWSKI

Gefährliche Dateitypen

Wir haben für Sie eine Liste der Dateien zusammengestellt, die potenziell Viren enthalten können.

Dateitypen, die Viren enthalten können

Beschreibung	Dateiendung unter Windows
Diese Dateien werden von Windows direkt ausgeführt und können Viren oder Trojaner enthalten.	COM, EXE, SCR, BAT, CMD, PIF, LNK, HTA, HTM(L), VBS, VBE, JS, JSE, VXD, CHM, EML

Dateitypen, die Makroviren enthalten können

Beschreibung	Dateiendung unter Windows
Microsoft-Office-Dateien können Makroviren enthalten.	DOC, XLS, PPT, PPS, MDB

Dateitypen, die bislang als sicher galten

Beschreibung	Dateiendung unter Windows
Diese beiden galten lange als sicher, können aber mittlerweile auch Würmer enthalten.	PDF, RTF

4 SYMANTEC-WEBSEITE Der Antiviren-Software-Hersteller Symantec bietet auch online Sicherheitschecks für Ihren Computer.

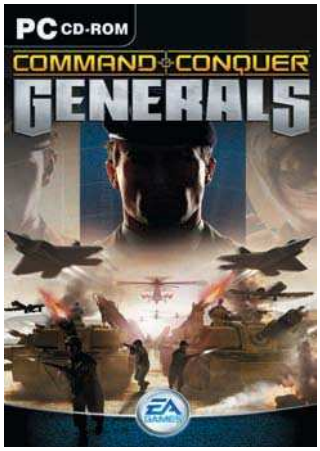
5 FIREWALL Installieren Sie unbedingt eine Firewall. Sie verhindert, dass schädlicher Code erst gar nicht auf Ihren Rechner kommt.

Webseiten

Virenschutz: Antivir 6 Personal Edition – www.free-av.de/F-Prot Anti Virus – www.f-prot.com/ Kaspersky Anti Virus Pro – www.kaspersky.com
Trojanerschutz: Zone Alarm – www.zonelabs.com/Sygate Personal Firewall – www.sygate.com/ Anti Trojan Shield – www.atshield.com

Angriff der Spitzen-Prämien

So viele Prämien gab's noch nie bei PC Games Hardware. Wer jetzt einen neuen Abonnenten wirbt, hat die Qual der Wahl unter **reihenweise genialen Prämien.**



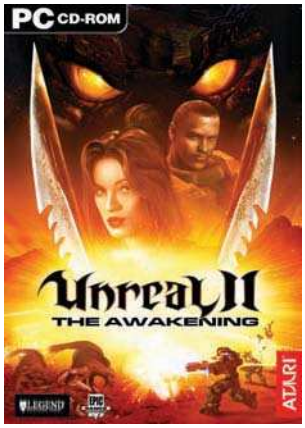
Command & Conquer: Generals
Im neuesten Spross der *C&C*-Serie kämpfen Sie auf Seiten der chinesischen Armee, den Vereinigten Staaten und einer augenscheinlich terroristischen Organisation namens GLA in insgesamt 27 Missionen um die Weltherrschaft. Das Spiel bietet durch die 3D-Welten mehr spielerischen Tiefgang und optische Pracht.

Prämien-Nr.: 002104

Artec DVD-ROM 16x48x
Vorbei sind die langen Wartezeiten bei großen Installationen und Datentransfers. Das Artec DVD-ROM 16x48x hat im DVD-Modus eine durchschnittliche Transferrate von 10 MB/s - und das bei mittleren Zugriffszeiten von 117 Millisekunden. Es ist kompatibel mit alle gängigen DVD-Formaten und kann auch wiederbeschreibbare DVD-Medien lesen. Zudem ist das Laufwerk auch bei hohen Drehzahlen relativ leise.

Prämien-Nr.: 002215

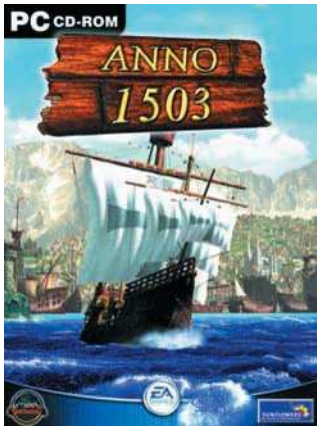
abo.pcgameshardware.de +++ http://abo.pcgameshardware.de +++ http://abo.pcgameshardware.de +++ http://abo.pcgameshardware.de +++ http://abo.pcgameshardware.de +++



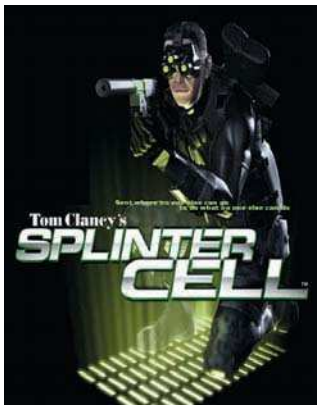
Unreal 2
Nachfolger des legendären Ego-Shooters von Epic Games mit grandioser Grafik.
Prämien-Nr.: 002197

Zalman ZM80-HP (A)
Mit diesem Passivkühler können Sie Ihre High-End-Grafikkarte ohne Geräuschbelästigung kühlen.
Prämien-Nr.: 002218

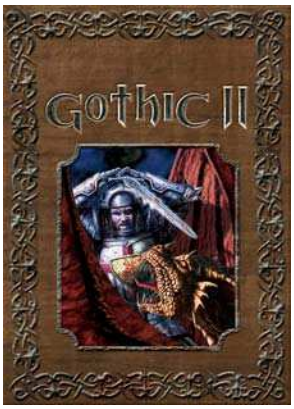
DTK USB-Stick 64 MB
Damit können Sie Daten, Bilder, MP3s immer bei sich führen und schnell auf andere PCs übertragen.
Prämien-Nr.: 002216



ANNO 1503
Stechen Sie in einer unbekannten Inselwelt in See. Langersehnter Nachfolger des Strategie-Klassikers.
Prämien-Nr.: 002086



Splinter Cell
Ein taktisches High-Tech-Action-Adventure der Extraklasse.
Prämien-Nr.: 002089



Gothic II
Der Nachfolger des großen 3D-Rollenspiels aus Deutschland.
Prämien-Nr.: 002082

Terratec Aureon 5.1 Fun
Mit dieser Soundkarte können Sie Computerspiele-Sound in Zukunft räumlich erleben.
Prämien-Nr.: 002219

Logitech MouseMan Dual Optical
Mit diesem Präzisionsnager bekommen Sie Ihre Spielgegner in den Griff.
Prämien-Nr.: 002155

Coupon ausgefüllt auf eine Postkarte kleben und ab damit an: PC Games Hardware, Abo-Service, Postfach 11 29, 23612 Stockelsdorf.

Einfach und bequem online abonnieren:

abo.pcgameshardware.de

Dort finden Sie auch eine Übersicht sämtlicher Abo-Angebote von PC Games Hardware und weiterer COMPUTEC-Magazine.

PC Games Hardware – TESTS ■ TIPPS ■ TUNING – DAS HARDWARE-MAGAZIN FÜR PC-SPIELER

Vertrauensgarantie: Diesen Auftrag kann ich ab Absendung (Poststempel) innerhalb von 14 Tagen ohne Begründung widerrufen. Die rechtzeitige Absendung (z. B. per Postkarte, Brief, E-Mail) an PC Games Hardware, Computec Abo-Service, Postfach 1129, 23612 Stockelsdorf oder computec.abo@pvz.de ist fristwahrend.

Dieses Angebot gilt leider nicht für Österreich!

Ja, ich möchte das 2-Jahres-PC-Games-Hardware-Abo mit CD-ROM!

(€ 86,40/24 Mon. (= € 3,60/Ausgabe); Ausland € 112,80/24 Mon.)

Adresse des neuen Abonnenten, an die auch die Abo-Rechnung geschickt wird (bitte in Druckbuchstaben ausfüllen):

Name, Vorname

Straße, Nr.

PLZ, Wohnort

Telefon-Nr./E-Mail *(für weitere Informationen)*

Die Prämie geht an folgende Adresse:

Name, Vorname

Straße, Nr.

PLZ, Wohnort

Telefon-Nr./E-Mail *(für weitere Informationen)*

Aus rechtlichen Gründen dürfen Prämienempfänger und neuer Abonnent nicht ein und dieselbe Person sein! Das Abo gilt für mindestens zwei Jahre und verlängert sich automatisch um ein Jahr, wenn nicht spätestens sechs Wochen vor Ablauf des Bezugszeitraumes gekündigt wird. Die Prämie geht erst nach Bezahlung der Rechnung zu. Das Abo-Angebot gilt nur für PC Games Hardware.

Bitte senden Sie mir folgende Prämie:

Prämie | Prämien-Nr.

ÜBRIGENS: Sie können sich auch von Personen, die PC Games Hardware selbst nicht abonniert haben, als Abonnent werben lassen!

Der neue Abonnent war in den letzten zwölf Monaten nicht Abonnent der PC Games Hardware.

Datum, Unterschrift des Abonnenten

Bitte beachten: Bei Bankeinzug erhalten Sie zusätzlich zwei Ausgaben kostenlos!

Gewünschte Zahlungsweise des Abos:

PH S0 02

❒ Bequem per Bankeinzug (Prämienlieferzeit ca. 2-3 Wochen)

Kreditinstitut: _____

Konto-Nr. | | | | | | | | | | |

Bankleitzahl: | | | | | | | | |

Kontoinhaber: _____

❒ Gegen Rechnung (Prämienlieferzeit ca. 6-8 Wochen)

+++ http://abo.pcgameshardware.de +++ http://abo.pcgameshardware.de +++ http://abo.pcgameshardware.de +++ http://abo.pcgameshardware.de +++ http://abo.pcgameshard

Tipps und Kniffe für ein sicheres XP

Sicherheits-Tuning für

Für Windows XP sind einige Sicherheitsregeln zu beachten, wenn Dateien und Ordner vor fremden Zugriffen geschützt werden sollen. Dies betrifft das System an sich, aber auch einzelne Systemprogramme.

Windows XP mag das bisher beste und effektivste Betriebssystem der gesamten Windows-Linie sein – in puncto Sicherheit mangelt es aber genauso wie bei den älteren Versionen. Grund dafür sind vor allem Internet Explorer und Outlook Express, die immer wieder Sicherheitsmängel aufweisen. Auch der Einsatz von Kleinnetzwerken im privaten Bereich kann ein hohes Sicherheitsrisiko darstellen. Dabei genügen oft ein paar kleine Einstellungen oder Änderungen am System, um die Gefahr durch Datenspione oder Viren wesentlich zu verringern. Meist sind es nur ein paar Mausklicks in der Systemsteuerung oder den Programmoptionen.

Gerade bei der Nutzung des Internet Explorers und von Outlook Express ist es wichtig, bestimmte Sicherheitsregeln zu beachten. Dazu gehört das stete Überprüfen der Einträge, aber auch das Zusammenspiel zwischen Internetzugang und Windows-System. Durch die offene Architektur der Internet- und Netzwerk-Ressourcen unter Windows XP ist das Einschleusen gefährlicher Codes für Hacker oder Virenprogrammierer kein großes Problem – nicht umsonst ist in einschlägigen Kreisen ein „Virus Construction Set“ im Umlauf, das immer wieder neue Ableger bekannter Viren entstehen lässt.

Tipp 1: WinXP-Updates installieren

SCHWIERIGKEIT: FÜR EINSTEIGER

Nutzen Sie die unter XP vorhandene automatische Installation von Updates. Microsoft stellt in regelmäßigen Abständen – vor allem nach dem Bekanntwerden neuer Sicherheitsprobleme – aktuelle Dateien zum Download zur Verfügung. Wenn Sie nicht sicher sind, ob Ihr Windows XP alle aktuellen Patches und Verbesserungen enthält, klicken Sie im Bereich „Arbeitsplatz“ auf den Eintrag „Systemsteuerung“ und dort unter der Rubrik „siehe auch“ auf „Windows-Update“. Über den Internetzugang baut XP dann eine Verbindung zum Download-Bereich für Updates von Microsoft auf. Dort können Sie „von Hand“ nach Updates suchen und auswählen, welche installiert werden sollen. Da einige der Updates sehr umfangreich sind, kann der Download je nach Verbindung und Server-Auslastung einige Zeit

WAS IST?

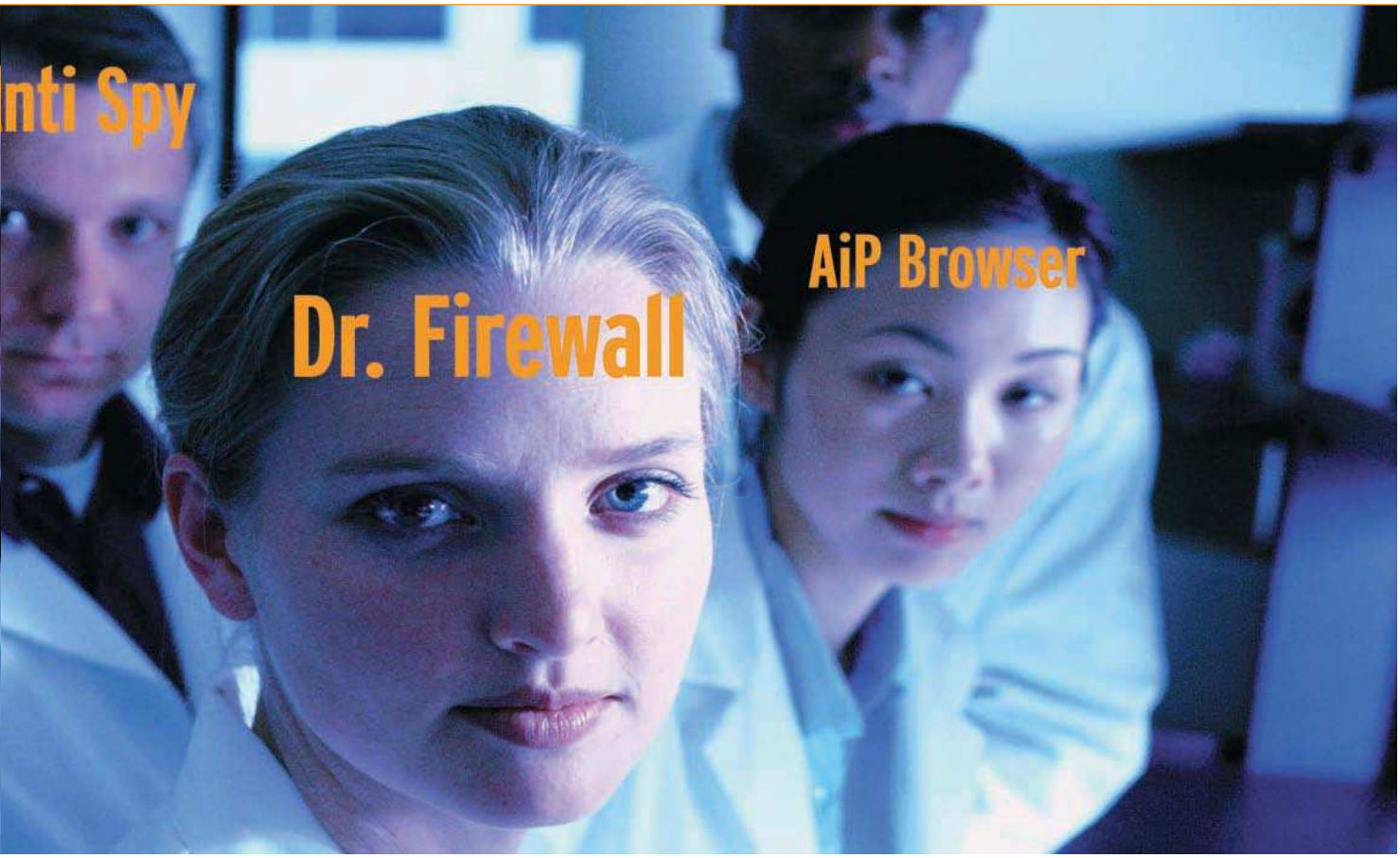
JavaScript/ActiveX
Spezielle weborientierte Computersprachen zur Steuerung dynamischer Inhalte.

Cookie
Kleine Textdatei, die Informationen über Aktionen und Steuerungen auf Webseiten enthält.

LAN
Lokales Netzwerk, bei dem alle Client-Rechner untereinander über Protokolle kommunizieren.

Trojanisches Pferd
Programm, das Schadprogramme wie Spion-Tools auf einem PC-System einschleust.

Windows XP



dauern. Windows unterbricht den Download, sobald keine Verbindung mehr besteht, setzt ihn aber fort, wenn eine neue Internetverbindung aufgebaut wurde. Sobald die Update-Dateien fertig geladen wurden, meldet der Update-Assistent, dass die Installation beginnen kann. Sie sollten auch – sofern noch nicht geschehen – das „Service Pack 1" zu Windows XP installieren. Dieses enthält Verbesserungen, Optimierungen und Fehlerkorrekturen zu Netzwerk- und Internetdiensten von Windows XP.

Tipp 2: IE – Temporären Speicher löschen

SCHWIERIGKEIT: FÜR EINSTEIGER

Nach jeder Verbindung im Internet ist es sinnvoll, den temporären Speicher des Browsers zu löschen. Der oft auch „Browser-Cache" genannte Ordner dient dazu, Seiten schneller aufzubauen, indem alle Seitenelemente, die nicht täglich aktualisiert werden, vom Browser direkt aus diesem Ordner heraus angezeigt werden. Durch diverse Tricks bei der Programmierung von Webseiten lassen sich die dort enthaltenen Daten aber dazu nutzen, den Besucher zu typisieren, zum Beispiel durch Rückverfolgung der vorher besuchten Webadressen, durch Setzen und Lesen von Cookies oder durch Platzieren kleiner Bilddateien, der „Web-Bugs".

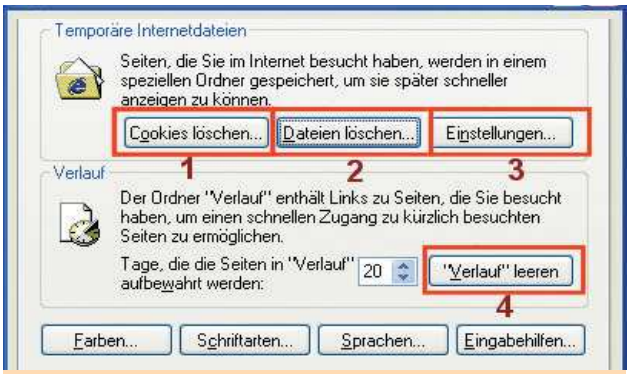
Wer sichergehen will, dass der Cache nicht für diese Zwecke genutzt wird, kann dies durch folgende Schritte verhindern: Rufen Sie entweder über das Browser-Menü „Extras" oder in der Systemsteuerung den Eintrag „Internetoptionen" auf. Nun klicken Sie die Buttons „Cookies löschen", wenn alle Cookie-Daten entfernt werden sollen, oder „Dateien löschen" und „Alle Offlineinhalte löschen", wenn alle temporären Dateien entfernt werden sollen, an. Über „Einstellungen…" und „Dateien anzeigen…" können Sie Daten im temporären Bereich einsehen. Durch Klicken von „,Verlauf leeren" werden die Einträge der zuletzt besuchten Webseiten gelöscht. Allerdings muss diese Aktion im Fall von mehreren Benutzern des Windows-XP-Rechners entweder komplett vom jeweiligen Systemadministrator für alle Benutzer oder von diesen selbst vorgenommen werden.

Tipp 3: Temporären Speicher verschieben

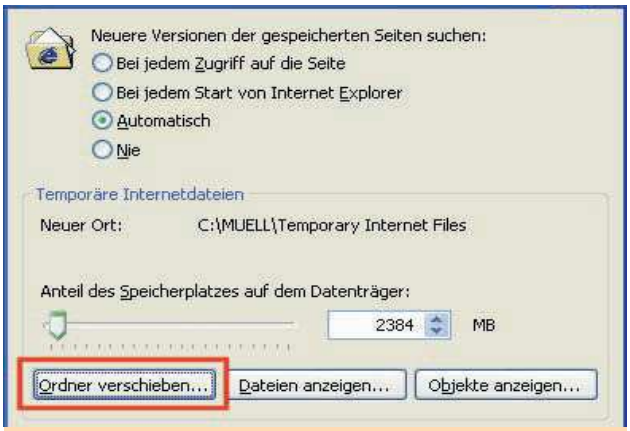
SCHWIERIGKEIT: FÜR EINSTEIGER

Viele der Seitenmechanismen im Internet nutzen die Bequemlichkeit der Windows-Benutzer aus, die vom System her vorgegebenen Einstellungen für Speicherorte dauerhaft zu übernehmen. Beim temporären Speicher zielen die Ausleseversuche meist auf den Ordner für „Temporäre Internetdateien" in den Userprofilen. Wenn Sie es potenziellen Spionen auf besuchten Webseiten schwer machen möchten, dann verschieben Sie den Ordner für die Temp-Dateien einfach an einen anderen Ort: Legen Sie auf einer Festplatte oder einer Partition ein neues Verzeichnis an (Beispiel „MUELL"). Nun wechseln Sie in die „Internetoptionen" und

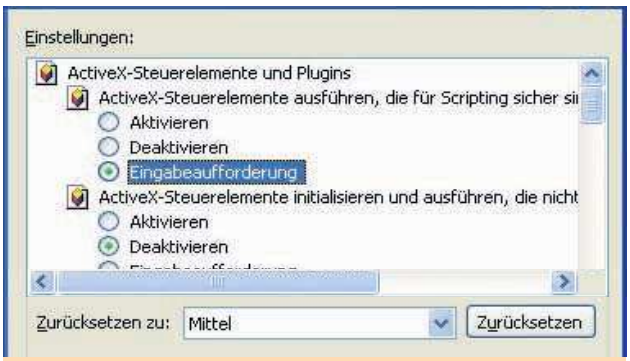
1 WINDOWS-UPDATE Um Sicherheitsprobleme unter XP zu vermeiden, sollten Sie grundsätzlich alle Updates zum System installieren.



2 BROWSERCACHE Einige wenige Schritte sind nötig, um den IE um einiges sicherer zu machen. Regelmäßige Updates sind zudem Pflicht!



3 VERSCHIEBEN Wird der Ordner für das Speichern der temporären Internetdateien geändert, können Spionageversuche ins Leere laufen.



4 ACTIVEX Hier stellen Sie ein, wie mit Webseitenkontrollen durch JavaScript oder ActiveX verfahren werden soll.

klicken dort den Button „Ordner verschieben“ an. Wählen Sie in der Ordnerauswahl den neu erstellten Ordner und klicken Sie auf „OK“. Von nun an werden temporäre Dateien und Cookies im neuen Verzeichnis gespeichert.

Tipp 4: ActiveX und JavaScript abschalten

SCHWIERIGKEIT: FÜR FORTGESCHRITTENE

Ein großes Problem des Internet Explorers ist die Kontrolle durch in Webseiten implementierten Programm-Code. Vor allem JavaScript und ActiveX-Controls sorgen immer wieder für Probleme beim Surfen im Internet. Dabei gibt es aber Unterschiede: JavaScript dient nur zur Steuerung bestimmter Abläufe, Viren können mit JavaScript alleine nicht realisiert werden. ActiveX dagegen – die Microsoft-Alternative – verfügt über Befehlsstrukturen, die einen direkten Eingriff in das lokale Windows-System des Benutzers ermöglichen. Damit dies verhindert wird, unterscheidet der Browser zwischen „vertrauenswürdigen“ und „nicht vertrauenswürdigen“ Codes auf einer Website – was allerdings keinerlei Garantie gibt, ob ein „vertrauenswürdiger Code“ nicht doch eine Gefahr für Ihren PC darstellt. Aus diesem Grund sollten Sie den Ablauf für JavaScript und ActiveX zur Sicherheit einschränken, vor allem wenn Sie im Internet unbekanntes Terrain betreten. Dazu gehen Sie wie folgt vor: Öffnen Sie die „Internetoptionen“. Wählen Sie die Registerkarte „Sicherheit“ aus. Klicken Sie nun auf den Button für „Stufe anpassen“. In den Einstellungen ändern Sie die Einträge für ActiveX- und JavaScript-Elemente, die standardmäßig auf „Aktivieren“ stehen, auf „Eingabeaufforderung“ um. Wird nun ein solches Element von einer Website aktiviert, so werden Sie gefragt, ob das Element gestartet werden soll oder ob Sie den Start ablehnen möchten.

Tipp 5: Bestimmte Cookies sperren/zulassen

SCHWIERIGKEIT: FÜR FORTGESCHRITTENE

Wird der temporäre Speicher des Browsers gelöscht, gehen unter Umständen auch Cookies von Webshops verloren, die man für den Datenaustausch (zum Beispiel eines Warenkorbes) benötigt. Andererseits möchten Sie vielleicht gleich dafür sorgen, dass bestimmte Websites keine Cookies setzen können. In diesem Fall rufen Sie die Cookie-Verwaltung des Internet Explorers auf. In den „Internetoptionen“ wechseln Sie in die Registerkarte „Datenschutz“. Dort klicken Sie auf den Button „Bearbeiten…“. Hier finden Sie die Cookie-Verwaltung des Browsers: Geben Sie im oberen Adressfeld die Webadressen der zu erlaubenden oder zu sperrenden Cookie-Versender ein. Über die Buttons „Sperren“ und „Zulassen“ vergeben Sie nun das Attribut „Immer sperren“ oder „Immer zulassen“ für die Website. So können Sie erwünschte Cookie-Daten erhalten, ohne unerwünschte Cookies mitzuspeichern.

Tipp 6: Media-Player-Spion deaktivieren

SCHWIERIGKEIT: FÜR EINSTEIGER

Der „Media Player“ von Windows kann ohne Kenntnis seines Benutzers Daten verschicken. So liefert der Player nicht nur die Informationen über jedes gespielte Musik- oder Videostück, er sendet zudem noch persönliche Daten über eine bestehende Internetverbindung. Um das zu unterbinden, müssen Sie im Player ein paar Einträge in den Optionen ändern: In der Registerkarte „Player“ sind die drei Einträge namens „Automatische Updates – Codecs automatisch downloaden“, „Interneteinstellungen – Identifikation des Players durch Internetsites zulassen“ sowie „Lizenzen automatisch erwerben“ durch Checkmarks aktiviert. Deaktivieren Sie diese drei Checkmarken durch Anklicken, danach klicken Sie auf den Button „Übernehmen“ oder „OK“. Jetzt ist der Player nur noch eingeschränkt in der Lage, Daten zu übermitteln.

Tipp 7: „XP-Antispy“ einsetzen

SCHWIERIGKEIT: FÜR EINSTEIGER

Da viele einzelne Komponenten von Windows XP für das Versenden von teilweise persönlichen Daten verantwortlich

sind und Einsteiger deshalb kaum eine Chance haben, alle versteckten Fallen von sich aus aufzufinden, empfiehlt sich der Einsatz eines kleinen, kostenlosen Programms namens „XP-Antispy“. Das nicht mal 100 Kilobyte große Programm lässt sich direkt von der Seite der Programmierer unter www.xp-antispy.de herunterladen und sofort einsetzen.

XP-Antispy zeigt alle vorhandenen Programmfunktionen auf, die direkt oder indirekt Sicherheitsprobleme erzeugen können. Hier finden sich nicht nur Einstellungen zur Systemkonfiguration von XP, sondern auch die eben schon genannten Einstellungen des Media Players sowie auch Start- und Endfunktionen, die unnötig Ressourcen belegen und den Rechner verlangsamen. Durch einfaches Setzen oder Löschen von Checkmarken oder Auswahlpunkten wird das System aktualisiert und die Start- oder Endfunktionen entsprechend geändert.

Tipp 8: XP-Nachrichtendienst abschalten

SCHWIERIGKEIT: FÜR FORTGESCHRITTENE

Der XP-Nachrichtendienst soll eigentlich in XP-Netzwerken die sofortige Übermittlung von Informationen zwischen den angeschlossenen Client-Rechnern ermöglichen. Durch spezielle Programmierung des Dienstes lassen sich aber auch Werbe-Mails („Spam“) auf mit dem Internet verbundenen XP-Computern einschleusen. Um dies zu verhindern, gehen Sie wie folgt vor:

Wählen Sie in der „Systemsteuerung“ den Eintrag „Verwaltung“ und nachfolgend den Eintrag „Dienste“. Im Übersichtsfenster suchen Sie nun den Eintrag „Nachrichtendienst“. Klicken Sie ihn mit der rechten Maustaste an. Im daraufhin erscheinenden Kontextmenü wählen Sie nun den Eintrag „Eigenschaften“. Im Eigenschaftsfenster müssen Sie den Eintrag „Starttyp“ auf „Deaktiviert“ setzen. Wenn Sie den Dialog nun mit „Beenden“ verlassen, ist der Nachrichtendienst beim nächsten Hochfahren des PCs abgeschaltet. Durch die gleichen Einstellungsbereiche können Sie den Dienst natürlich auch wieder aktivieren.

Tipp 9: Kennwörter nicht speichern

SCHWIERIGKEIT: FÜR EINSTEIGER

Bei der Verwaltung von Usernamen und Pass-/Kennwörtern zeigen manche XP-Benutzer immer noch eine erstaunliche Gelassenheit: Da wird ein- und dasselbe Passwort für mehrere Zugänge benutzt, Kennungen werden als Editor-Datei im Verzeichnis „Eigene Dateien“ abgelegt oder stehen jedem Benutzer des Rechners in Form von Einträgen in Dokumenten offen. Gerade solche Daten sind ein gefundenes Fressen für jeden Datenspion – und wer zusätzlich noch die TAN-Nummern seines Online-Kontos zusammen mit der PIN als nicht verschlüsselte Datei auf der Festplatte speichert, handelt höchst fahrlässig. Grundsätzlich gelten auf PCs – nicht nur auf Windows-Rechnern – die folgenden Regeln: Jeder Benutzer sollte ein eigenständiges Passwort erhalten. Außerdem sollte jedes Passwort eine willkürliche Zusammenstellung von Ziffern und Buchstaben und zudem noch eine Mischung aus Groß- und Kleinschreibung sein. „A7M12kf498“ ist in jedem Fall besser als „GERLINDE“ oder „waldi“. Grundsätzlich ist es ratsam, keine Passwörter auf dem PC zu speichern, entfernen Sie auch das Zugangspasswort für den Internetzugang beim Anwahlsystem (Eigenschaften der DFÜ-Verbindung aufrufen) und das Postfach-Kennwort für Ihr E-Mail-Konto unter Outlook Express. In jedem Fall sollte unter Windows XP immer ein Administrator-Eintrag vorhanden sein, da der Administrator über die komplette Rechtevergabe für alle Benutzer verfügen kann.

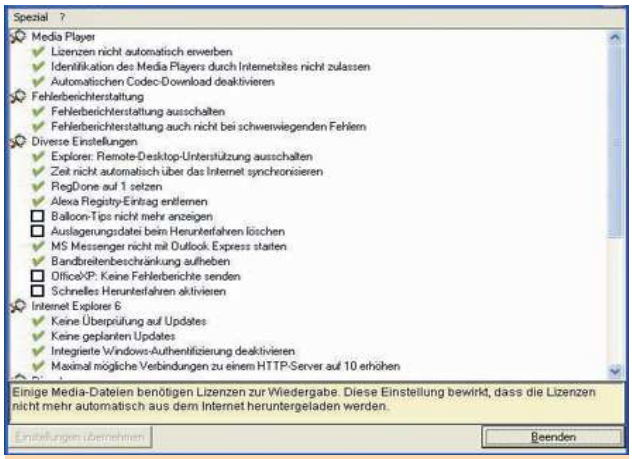
Tipp 10: Keine Datei- und Druckerfreigabe!

SCHWIERIGKEIT: FÜR FORTGESCHRITTENE

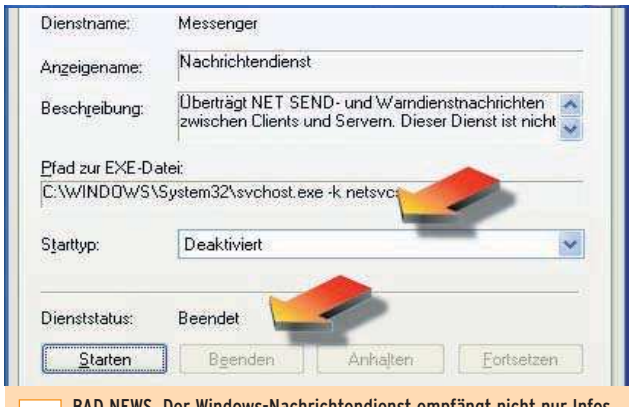
Ist unter Windows XP ein Netzwerk eingerichtet – zum Beispiel, wenn ein neuer PC angeschafft wurde, der alte jedoch als Druck- und Datei-Server dienen soll –, dann wird bei der Installation des Netzwerks von XP aus meist eine Netzwerkinstal-

5 COOKIE-VERWALTUNG Welche Cookies erhalten bleiben sollen, lässt sich sich über „Sperren“ und „Zulassen“ festlegen.

6 DATENSCHLEUDER Durch Ändern der drei Kontrolleinträge verhindern Sie, dass der Media Player ungefragt persönliche Daten übermittelt.

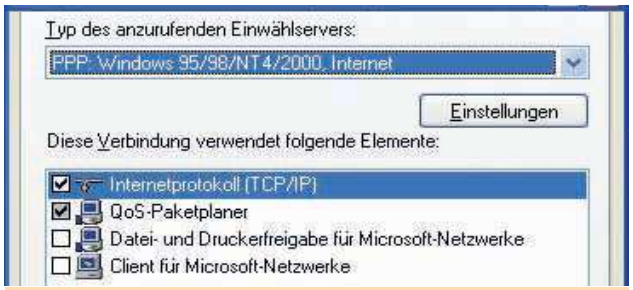


7 XP-ANTISPY Mit XP-Antispy lassen sich viele Einstellungen zu komfortabel setzen oder löschen, die manuell sehr zeitaufwendig wären.

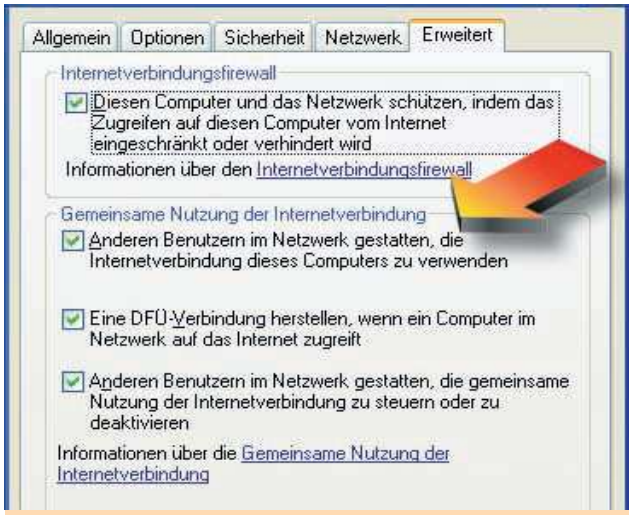


8 BAD NEWS Der Windows-Nachrichtendienst empfängt nicht nur Infos und Texte, sondern auch Werbebotschaften aus dem Internet.

9 **PASSWORT** E-Mail-Konten werden meist mit gespeichertem Passwort eingerichtet. Sicherer ist es aber, das Passwort zu speichern.



10 **FREIGABEN** Durch die „Datei- und Druckerfreigabe" werden potenziellen Angreifern aus dem Internet Tür und Tor geöffnet.



11 **VERBINDUNGSZUGRIFF** Soll eine Internetverbindung lokal nur vom Administrator verwaltet werden, bedarf es bestimmter Einstellungen.

12 **FIREWALL** Die XP-Firewall bietet nur mäßigen Schutz. Soll eine externe Firewall eingesetzt werden, sollten Sie die interne abschalten.

lationsdiskette genutzt, welche die Einstellungen für das Netzwerk auf alle angeschlossenen Rechner übertragen kann. Dabei wird die „Datei- und Druckerfreigabe" als Dienst mitinstalliert. Diese steht allerdings dann nicht nur dem LAN (Local Area Network) zur Verfügung, sondern auch dem Internetdienst, sofern dieser ebenfalls eingerichtet ist. Freigegebene Ordner, Festplatten oder Partitionen sind damit für potenzielle Datendiebe im Internet ein gefundenes Fressen. Um die Datei- und Druckfreigabe für das Internet abzuschalten, gehen Sie wie folgt vor: Öffnen Sie „Arbeitsplatz", „Netzwerkumgebung" und „Netzwerkverbindungen anzeigen". Wählen Sie im Bereich „DFÜ" oder „Netzwerkbrücke" den genutzten Internetzugang. Mit der rechten Maustaste öffnen Sie nun die „Eigenschaften". In der Registerkarte „Netzwerk" finden Sie den Untereintrag „Diese Verbindung verwendet …", darunter befinden sich Checkmarken für die verwendeten Dienste. Entfernen Sie die Checkmarke bei „Datei- und Druckerfreigabe für Microsoft-Netzwerke" und klicken Sie auf „OK". Damit ist die Freigabe für die Internetverbindung abgeschaltet.

Tipp 11: Schutz der Internetverbindung

SCHWIERIGKEIT: FÜR FORTGESCHRITTENE

Wird ein XP-Computernetzwerk in mehreren vernetzten Rechnern eingesetzt, aber nur einer der angeschlossenen PCs verfügt über einen Internetzugang, dann wird dieser Zugang vom System standardmäßig für alle Benutzer freigeschaltet. Dies betrifft auch Änderungen an den Zugangseinstellungen für den DFÜ-Dienst. Um das zu unterbinden, wechseln Sie noch einmal in die Eigenschaften des Internetzugangs. Unter der Registerkarte „Gemeinsame Nutzung…" finden Sie drei Einträge:

„Anderen Benutzern im Netzwerk gestatten …" bedeutet: Ist hier die Checkmarke gesetzt, wird die Internetverbindung im Netzwerk freigeschaltet, andernfalls sperrt der lokale Rechner den Zugang für das Netzwerk. „Eine DFÜ-Verbindung herstellen …" bedeutet: Meldet bei gesetzter Checkmarke ein Netzwerkrechner eine Internetverbindung an, wobei als Internetzugang die „LAN-Verbindung" eingerichtet sein muss, wählt der lokale Computer sich ohne Rückfrage im Internet ein. „Anderen Benutzern im Netzwerk gestatten …" bedeutet: Jeder Netzwerkrechner kann eine Anforderung an den lokalen Computer übermitteln, mit der Änderungen am Internetzugang vorgenommen werden können. Durch Löschen der entsprechenden Checkmarke können Sie dafür sorgen, dass Sie als Administrator den kompletten Zugriff auf das Internet kontrollieren können – vorausgesetzt, Sie haben sich als Administrator mit Passwort in das System eingeloggt.

Tipp 12: Interne Firewall abschalten

SCHWIERIGKEIT: FÜR FORTGESCHRITTENE

In der gleichen Registerkarte finden Sie oben den Eintrag „Internetverbindungsfirewall". Die Internet-Firewall von Windows XP schützt nur sehr eingeschränkt, da sie zwar den Datenverkehr von „draußen" zum lokalen Rechner beobachtet, nicht aber den Datenverkehr vom Rechner ins Internet – ist ein „Trojanisches Pferd" oder ein „Remote-Control-System" installiert, versendet es persönliche Daten, ohne dass die Firewall dies registriert. Zudem protokolliert die Firewall die Vorgänge beim Datenaustausch von „draußen nach drinnen" nur unzureichend, was eine genaue Verifizierung von Zugriffen erschwert.

Wer eine externe Firewall einsetzen möchte, zum Beispiel die hervorragende kostenlose Firewall „Zonealarm" von der amerikanischen Firma Zone Labs (www.zonelabs.com) oder kommerzielle wie die Firewall-Systeme von McAfee oder Norton, sollte die XP-interne Firewall abschalten. Dazu klicken Sie einfach das Kontrollkästchen in der Registerkarte an. Damit kann ein externes Firewall-System ungehindert die Protokollierung übernehmen.

JÜRGEN BORNGIESSER

ideenhaus muc

DIE WELT DES FILMS HAT VIELE SEITEN.

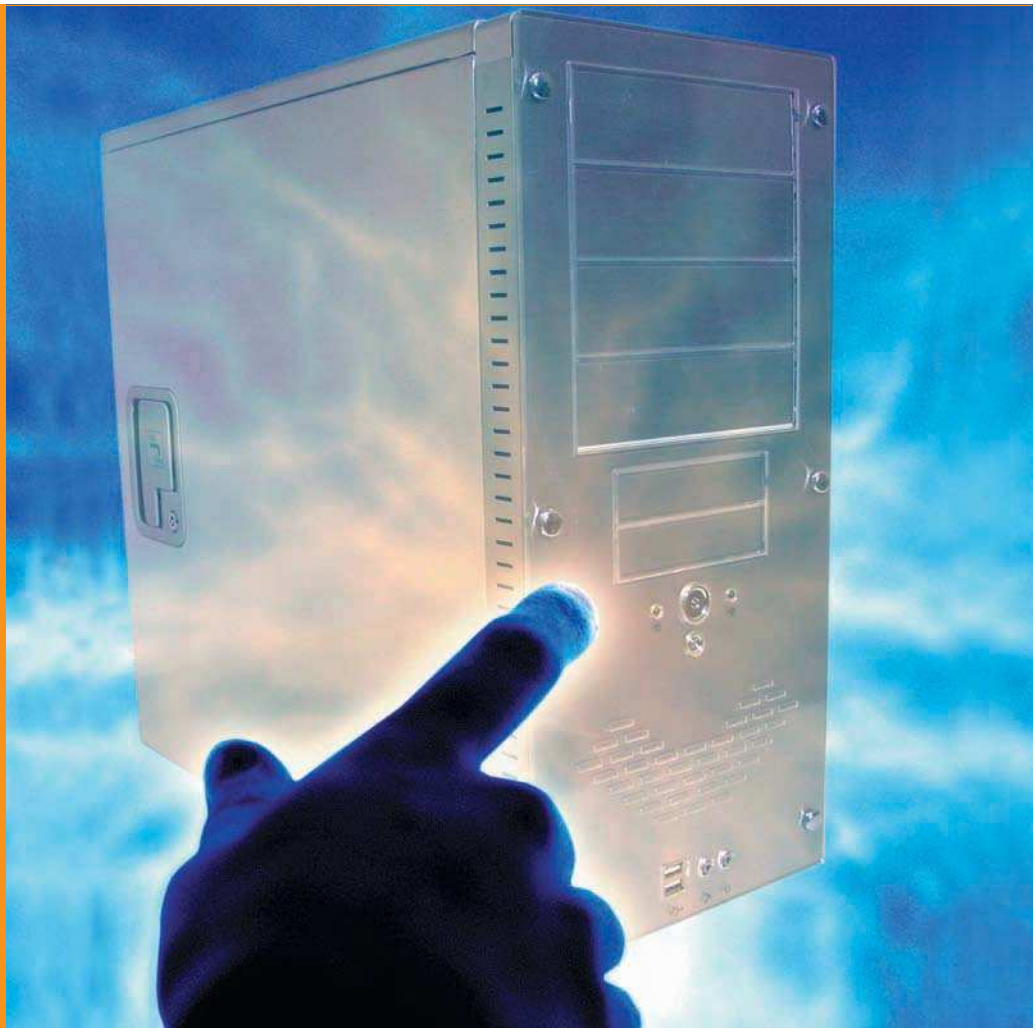
Sieh an: mit DVD!
Trailer, Reportagen, Features,
Tests u. v. m.

JETZT NEU: DAS GROSSE MAGAZIN FÜR FILMFANS. ||| MIT KINO, DVD, TECHNIK UND MEHR. ||| AB SOFORT FÜR NUR 3,99 EURO MIT DVD.

Workshop mit Zone Alarm

Schutzschild für den PC

Der Einsatz einer Firewall empfiehlt sich grundsätzlich dann, wenn ein PC mit dem Internet verbunden ist. Zone-Alarm bietet bestmöglichen Schutz vor Datenspionen und Hacker-Attacken und ist zudem kostenlos.



Wird ein Computer über eine Datenleitung mit dem Internet verbunden, besteht schnell die Gefahr, dass sensible und persönliche Daten frei zugänglich sind. Dabei ist völlig unerheblich, welche Verbindungsart man wählt. Ob Modem, ISDN, DSL oder Netzwerksystem: Wenn die Daten nicht zusätzlich abgesichert sind, können Datenspione mit nur wenigen Hand- und Programmiergriffen zielsicher zugreifen. Hier empfiehlt sich der Einsatz einer Firewall, einer „Brandschutzmauer“, die Attacken aus dem Internet abwehren kann. Die in Windows XP integrierte Firewall ist da keine große Hilfe, besser ist der Einsatz eines externen Systems. „Zone Alarm“ ist zwar ein englischsprachiges Produkt, die Konfiguration des Programms ist aber denkbar einfach. Wir zeigen Ihnen die wichtigsten Einstellungen für besten Schutz.

Tipp 1: Zone Alarm muss erst lernen

SCHWIERIGKEIT: FÜR EINSTEIGER

Zone Alarm ist wie andere Firewall-Systeme eine Hilfe gegen Angriffe von außen. Das bedeutet jedoch nicht, dass Ihr PC ab dem Moment des ersten Startens einer Firewall gegen alles und jeden abgesichert ist. Stattdessen muss jede Firewall erst einmal „lernen“, wie Ihr PC funktioniert und welche Programme Sie nutzen. Eine Firewall soll genehmigte Prozesse und Verbindungen vom und zum Internet (oder Netzwerk) zulassen, nicht genehmigte aber abblocken. Ansonsten könnten Sie zum Beispiel keine E-Mails empfangen oder senden.

Deshalb startet jedes Firewall-System mit einer Erfassung der Programme, die für den Internetzugang gedacht sind: Browser, E-Mail-Client, FTP-Client und Ähnliches. Jedes weitere

WAS IST?

Port
Speicheradressen im PC, über die Daten zwischen PC und Internet oder Netzwerk gesendet werden

FTP-Client
Programm zur Übermittlung von Daten und Dateien per „File Transfer Protocol“

Tracking
Methode, um einen Hacker anhand seiner Spuren im Internet zu identifizieren

Zone
Bereich innerhalb eines Netzwerks, der einen besonderen Status erhält (z. B. „sicher“)

Programm, zum Beispiel die Online-Registrierung einer Applikation, bleibt dagegen erst einmal unbeachtet – bis diese sich aktiviert. Da ein Firewall-System jede Datenübertragung zwischen lokalem Rechner und Netzwerk (auch Internet) über die Ports registriert, schaltet sich das System in genau diesem Moment ein, blockiert den Vorgang, informiert Sie darüber und wartet auf Ihre Entscheidung, was „jetzt" und „in Zukunft" damit passieren soll. Wenn Sie jetzt nicht wissen, was dieser Prozess bewirkt, und diesen deshalb ablehnen, fragt die Firewall beim nächsten Zugriff der Applikation auf die Internet-Ressourcen wieder nach – sofern Sie den Prozess nicht dauerhaft abgelehnt haben.

Wird dieser Prozess mehrmals in zeitlichen Abständen aktiviert, lässt sich der Vorgang automatisch regeln: Sie sagen der Firewall durch explizite Einstellungen, dass der Prozess genehmigt oder nicht genehmigt ist. Dann legen Sie im Fall einer Genehmigung fest, wie der Prozess arbeiten darf: Wird ein spezieller Port benutzt oder sind es mehrere? Dürfen Daten verschickt und empfangen werden? Dürfen versteckte Prozesse automatisch weitere Unterroutinen aufrufen, die ebenfalls Zugriff erhalten?

Nach und nach erweitern Sie so die Zugriffsregeln der Firewall, bis diese automatisch auf die meisten Vorgänge reagieren kann. Das bedeutet allerdings auch, dass eine Firewall keine „Wunderwaffe" ist. Die erste Zeit mit einer Firewall wird anstrengend, da fast keine Aktion ohne Nachfrage stattfindet – und das kann mitunter zur Geduldsprobe werden.

Tipp 2: Standard versus Professional

SCHWIERIGKEIT: FÜR EINSTEIGER

Auf der Website von Zone Labs, Inc. (www.zonelabs.com) findet sich im Download-Bereich neben der kostenlosen Standard-Variante der Firewall noch eine Trial- (Test-)Version der „ZoneAlarm Pro"-Version. Diese können Sie ebenfalls kostenlos herunterladen, sie steht Ihnen allerdings nur 30 Tage zur Verfügung und muss dann gegen Gebühr registriert werden. In diesem Workshop soll es jedoch um die dauerhaft nutzbare Standardversion gehen. Dabei sind folgende Punkte zu beachten: Erstens: Die Standardversion besitzt nur einen einfachen E-Mail-Scanner, das heißt, dass Ihr E-Mail-Postfach zwar auf schädlichen Code in Attachment-Dateien überprüft wird, aber keinen Rundumschutz gegen Würmer oder Script-Viren besitzt. Sie sollten daher unbedingt einen externen Virenscanner installieren. Zweitens: Eine Zurückverfolgung von Hackerangriffen („Tracking") ist in der Standardversion nicht möglich. „Ad"- und „Pop-Up"-Kontrollen gegen Spionsoftware ist nicht integriert. Hier empfiehlt sich der zusätzliche Einsatz einer entsprechenden Software, zum Beispiel „Ad-Aware" unter www.lavasoftusa.com.

Tipp 3: Windows-XP-Firewall abschalten

SCHWIERIGKEIT: FÜR EINSTEIGER

Wenn Sie Zone Alarm unter Windows XP einsetzen möchten, sollten Sie die integrierte Firewall abschalten, da beide Firewall-Systeme ansonsten Probleme miteinander bekommen. Dazu wählen Sie einfach die Netzwerk-Ressource, zum Beispiel für den Internetzugang, klicken mit der rechten Maustaste auf das Symbol, um das Kontextmenü aufzurufen, und dann auf die „Eigenschaften". In der Registerkarte „Erweitert" löschen Sie das Häkchen für die Verbindungs-Firewall.

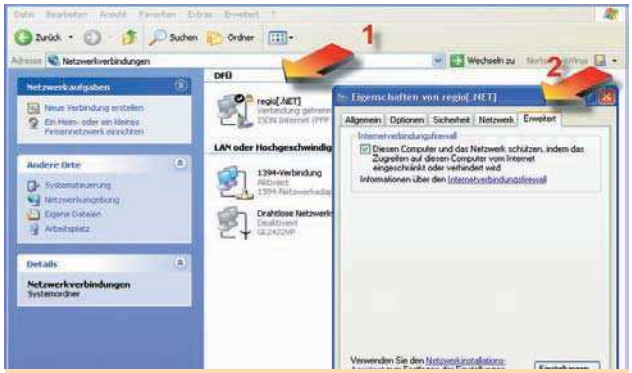
Tipp 4: Grundsätzliche Einstellungen setzen

SCHWIERIGKEIT: FÜR EINSTEIGER

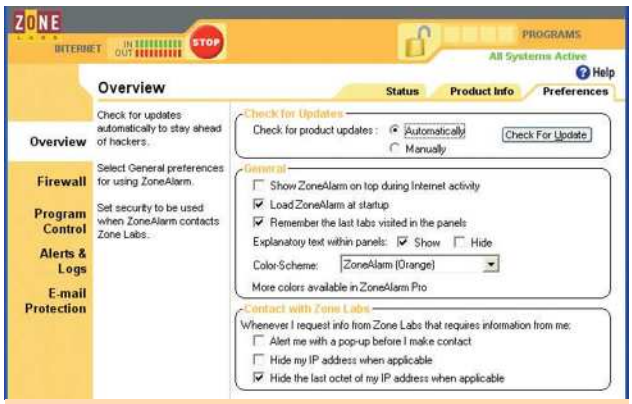
Zone Alarm beobachtet jedes auf Ihrer Festplatte befindliche Programm auf Verbindungsaktivität. Wenn ZoneAlarm installiert wird, fragt es den Benutzer zuerst, wann es Blockierungen der Netzwerkzugriffe anzeigen soll. Die Einstellung „Don't alert me at all …" bedeutet, dass Zone Alarm die meisten Protokollierungen und Blockierungen ohne Information und automatisch ablaufen lässt. Besser ist jedoch die Einstellung „Alert me whenever …" – hier zeigt Zone-

Your computing environment:	ZoneAlarm Pro	ZoneAlarm Plus	ZoneAlarm
My PC is used for personal purposes	✔	✔	✔
My PC is a desktop	✔	✔	✔
Your security priorities:	**ZoneAlarm Pro**	**ZoneAlarm Plus**	**ZoneAlarm**
Strong firewall	✔	✔	✔
Protect against email borne viruses and worms	✔	✔	✗
Up-to-the-minute information on threats to my PCs security	✔	✔	✔
Track and map suspected hackers to determine the source of attacks	✔	✔	✗
Protect my privacy online by controlling cookies	✔	✗	✗
Control over ads and stop pop-up windows	✔	✗	✗
Control mobile code (JavaScript, ActiveX) that websites try to run on my PC	✔	✗	✗
Technical support available	✔	✔	✗
Our recommendation	★★★★★	★★★	★★

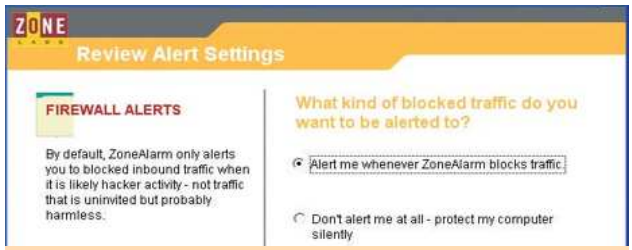
2 VERSIONEN Auf der Website von Zone Labs informiert diese Übersicht über die Funktionen der jeweiligen ZoneAlarm-Versionen.



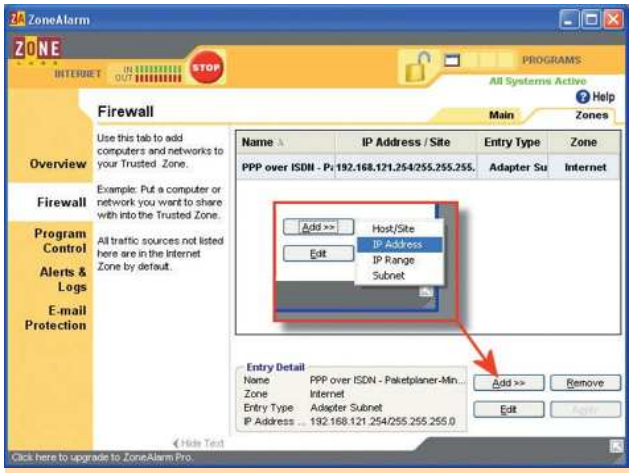
3 XP-FIREWALL Bei Windows XP ist es beim Einsatz von Zone Alarm ratsam, die integrierte Firewall abzuschalten.



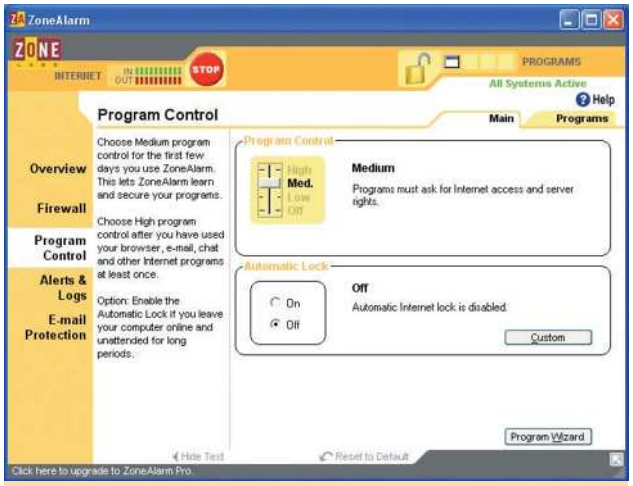
4 GRUNDEINSTELLUNGEN Unter „Overview" finden Sie den internen Update-Check sowie grundsätzliche Einstellungen für den Start.



4 MELDEPFLICHT Nach der Installation fragt Zone Alarm, wie oft es Vorgänge melden soll und welche Programme geblockt werden sollen.



6 DATENBANK In den „Zones" finden Sie automatisch eingetragene Applikationen, können diese aber auch selbst festlegen.



7 INFORMATION In der Programmkontrolle legen Sie fest, wie Programme verfahren sollen, wenn sie eine Internetverbindung anfordern.

7 HANDARBEIT Sie können die Verfahrensweise für Verbindungsanforderungen von Programmen auch gesondert festlegen.

Alarm jede Aktivität an und lässt den Benutzer entscheiden, ob es dem jeweiligen Programm Zugriffe auf Internetressourcen erlauben soll oder nicht. Zwar sind die vielen „Alerts" (Alarmmeldungen) anfangs etwas nervig, mit der Zeit selektiert man aber so den Zugriff und lernt, wie ZoneAlarm als Firewall arbeitet. Die Einstellung kann später allerdings jederzeit auch geändert werden.

Die zweite Grundeinstellung betrifft das Einbringen bekannter Applikationen wie Webbrowser in die Aktivitätsliste. Die Auswahl „Yes" sorgt dafür, dass ZoneAlarm sofort diese bekannten Applikationen integriert. Ansonsten wird jeder spätere Internetzugriff erst über ZoneAlarm gelenkt, bis die Eintragungen von Ihnen bestätigt wurden.

Tipp 5: Programmeinstellungen vornehmen

SCHWIERIGKEIT: FÜR EINSTEIGER

Nach dem Start von ZoneAlarm müssen Sie das Piktogramm in der Taskleiste anklicken, damit sich das Hauptfenster öffnet. Klicken Sie nun auf den Bereich „Overview" (Übersicht) und hier auf die „Preferences" (Voreinstellungen). Hier finden Sie die Programmeinstellungen: „Check for Updates" sollte auf dem Eintrag „Automatically" stehen, damit Zone Alarm überprüfen kann, ob neue Updates auf dem eigenen Webserver vorhanden sind.

„General": Hier sollte der Eintrag „Load Zone Alarm at startup" markiert sein, damit die Firewall automatisch mit dem Windows-Start aktiviert wird.
„Contact with Zone Labs": Interessanterweise hilft Hersteller ZoneLabs dem Anwender, seine Daten vor Zone Labs selbst geheim zu halten. Die drei Checkmarken bedeuten: „Alert me with a popup …". Hier wird vor einer Verbindung nach ZoneLabs mit einem Pop-up-Window aufmerksam gemacht. „Hide my IP-address …". Wird eine Verbindung nach ZoneLabs aufgebaut, übermittelt die Firewall nicht die eigene IP-Adresse, hier sollte man einen Haken setzen, sofern die Verbindung nicht über einen Proxy-Server stattfindet. Damit verhindert man das Übersenden der eigenen IP an ZoneLabs. „Hide the last octet …". Diese Funktion ist voreingestellt, hier entfernt Zone Alarm die letzten Kennziffern der IP-Nummer.

Tipp 6: Netzwerk-Adressen eintragen

SCHWIERIGKEIT: FÜR FORTGESCHRITTENE

Wird eine Internetverbindung über ein Netzwerk eingerichtet oder ist der lokale PC-Teil eines Heimnetzwerks, muss sichergestellt sein, dass die am Netzwerk angeschlossenen Rechner von ZoneAlarm als „vertrauenswürdig" („trusted") erkannt werden. Im günstigsten Fall erkennt Zone Alarm automatisch, ob sich Rechner im Netzwerk befinden und ob diese über eindeutige IP-Adressen angemeldet sind. Ist dies nicht der Fall, müssen Sie die Rechner manuell erfassen. Gleiches gilt für Netzwerk-Ressourcen mit Internetverbindung, so sind diverse externe ISDN-Anlagen mit USB-Anschluss als Netzwerkgerät in Windows eingebunden. In diesem Fall wechseln Sie im Hauptfenster von ZoneAlarm in den Bereich „Firewall" und die Registerkarte „Zones". Über den Button „Add" können Sie auswählen, ob Sie eine Website (URL), eine IP-Adresse oder -Gruppe oder eine Subnetz-Maske eintragen möchten. Über eine IP-Adresse geben Sie zum Beispiel einen Netzwerkrechner an, über eine URL eine feste Webadresse. Achten Sie darauf, wie Windows die Netzwerk-Ressourcen eingerichtet hat, und geben Sie die Adressdaten genau an.

Tipp 7: Einstellung der Programmkontrolle

SCHWIERIGKEIT: FÜR EINSTEIGER

Jeder Applikation kann eine separate Konfiguration unter Zone Alarm zugewiesen werden. Wechseln Sie dazu in den Bereich „Program Control" und die Registerkarte „Programs". Hier sehen Sie alle Programme, die ZoneAlarm im Lauf der Zeit integriert hat. Jedem Programm werden die jeweiligen Rechte für „Zugriff" („Access") und Server, also lokale Dienste, gewährt. Durch Anklicken der Pik-

togramme für die Rechte, bestehend aus „Fragezeichen“ (Nachfrage bei jedem Zugriff), „Häkchen“ (freier Zugriff) oder „Kreuz“ (kein Zugriff), wird vom Benutzer entschieden, welches Programm wie behandelt werden soll. Wenn Sie sich nicht sicher sind, sollten Sie öfters das Fragezeichen setzen, dann sehen Sie, wann das entsprechende Programm Zugriff auf Internet oder lokale Bereiche nehmen will. Bei Programmen, deren Internetzugriff bekannt ist, also Webbrowser oder E-Mail-Client, können Sie die Rechte freigeben, sie werden von der Firewall immer noch auf „außergewöhnliche Umstände“ untersucht, also Zugriffe auf nicht benötigte Ports etc. Durch den Button „Add“ können Sie jederzeit neue, frei definierbare Applikationen hinzufügen. Wenn Sie zum Beispiel nicht sicher sind, ob Ihr neues Grafikprogramm nicht doch mehr Daten als die Registrierung über das Internet verschicken will, legen Sie es in der Liste ab und versehen Sie die Zugriffsrechte mit „Fragezeichen“. So meldet Zone Alarm jeden Zugriff dieses Programms.

Tipp 8: Überprüfen der gemeldeten Zugriffe

SCHWIERIGKEIT: FÜR FORTGESCHRITTENE

Wenn Sie den Bereich „Alerts&Logs“ auf der Hauptseite anklicken und in die Registerkarte „Log Viewer“ gehen, dann sehen Sie hier eine Log-Liste, in der jedes Programm, das einen Zugriff auf das DFÜ- oder lokale Netzwerk versucht, eingetragen wird. Anhand der Log-Liste stellen Sie fest, welche Programme in welchen Abständen versuchen, diese Verbindung aufzubauen. Jeder Eintrag kann mit der Maus markiert und aktiviert werden. Wenn Sie hier Einträge finden, die sich nicht anhand der Rechtevergabe klassifizieren lassen, müssen Sie anhand des Eintrags feststellen, woher oder wohin die Daten geschickt wurden. Ist eine Identifizierung möglich, erlaubt ZoneAlarm über den Button „Add to zone …“ eine Änderung des Status, so dass abgeblockte Daten für die Zukunft freigegeben werden können. Im Normalfall ist dies allerdings nur dann notwendig, wenn ZoneAlarm von sich aus nicht in der Lage ist, die Informationen über die Verbindung und den Datentransfer festzulegen.

Tipp 9: Das Internet blockieren

SCHWIERIGKEIT: FÜR EINSTEIGER

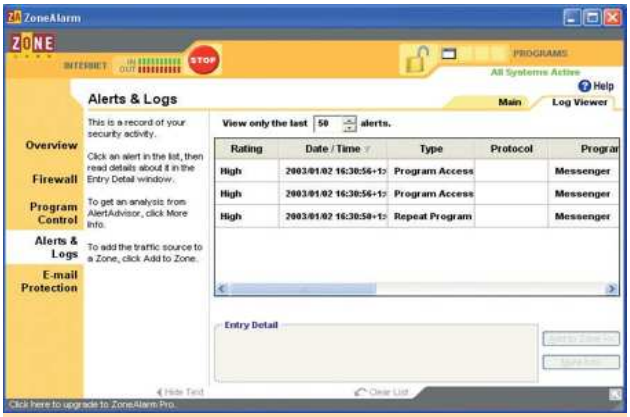
Im oberen Bereich des Hauptfensters sehen Sie eine kleine Grafik, die ein offenes Schloss zeigt. Wenn Sie hier mit der Maus klicken, schließt sich das Schloss, nochmaliges Klicken öffnet es wieder. Zusammen mit dem roten Stopp-Button daneben haben Sie hier eine direkte Kontrolle der Internetverbindung. Durch Klicken des Stopp-Buttons wird eine Verbindung sofort ohne Rücksicht auf Daten geschlossen, durch Anklicken des Schlosses („Lock“) wird jede Übertragung beendet, aber ohne die Verbindung zu kappen. Wenn Sie verhindern möchten, dass bestimmte Programme Zugriff erhalten, können Sie diese in der „Programmkontrolle“ ebenfalls mit einem Schloss („Lock“) versehen. Damit kann zum Beispiel der E-Mail-Empfang geöffnet bleiben, während der Browser gesperrt ist.

Tipp 10: Programme suchen

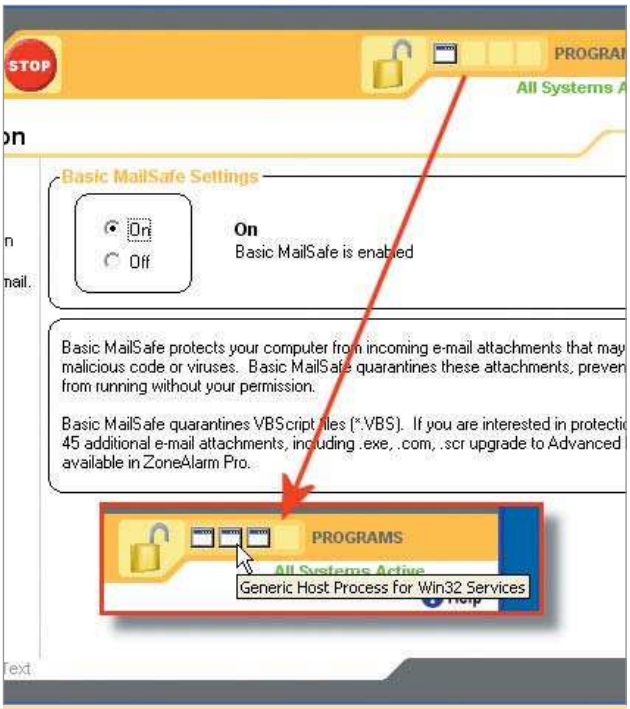
SCHWIERIGKEIT: FÜR EINSTEIGER

Zone Alarm meldet Zugriffe von Applikationen nicht nur mit den Alarmeinträgen, es zeigt auch den Originaldateinamen der Applikation an. Da diese aber oft nicht eindeutig einem Programm zugeordnet werden können, bietet es sich an, die Windows-Dateisuche mit einzubeziehen. Durch Eingabe des Dateinamens und der Suchaufforderung findet Windows den Ort, an dem die entsprechende Datei gespeichert ist. Eindeutige Ordner wie zum Beispiel für einen Virenscanner lassen darauf schließen, dass dieser seine Virendatenbank während einer Internetverbindung auf den neuesten Stand bringen will – ihn können Sie in der Rechtevergabe problemlos freischalten. Ist die Datei jedoch im Systemordner von Windows versteckt und ohne Verknüpfung zu wichtigen Programmen, ist Vorsicht angeraten. In diesem Fall sollten Sie die Datei für weitere Verbindungen sperren.

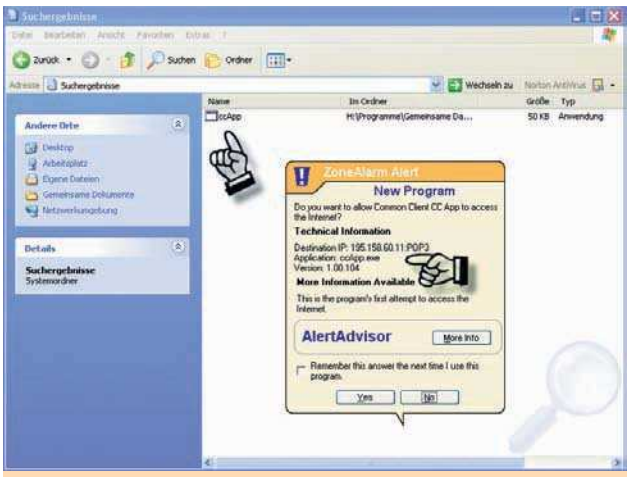
JÜRGEN BORNGIESSER



8 MELDELISTE Im Log-Viewer finden sich alle aufgelisteten Vorgänge, die ZoneAlarm in Verbindung mit Internetzugriffen registriert hat.



9 ÜBERWACHUNG Im Statusmonitor wird anzeigt, wie viele Programme einen Zugriff anfordern sowie weitere wichtige Informationen.

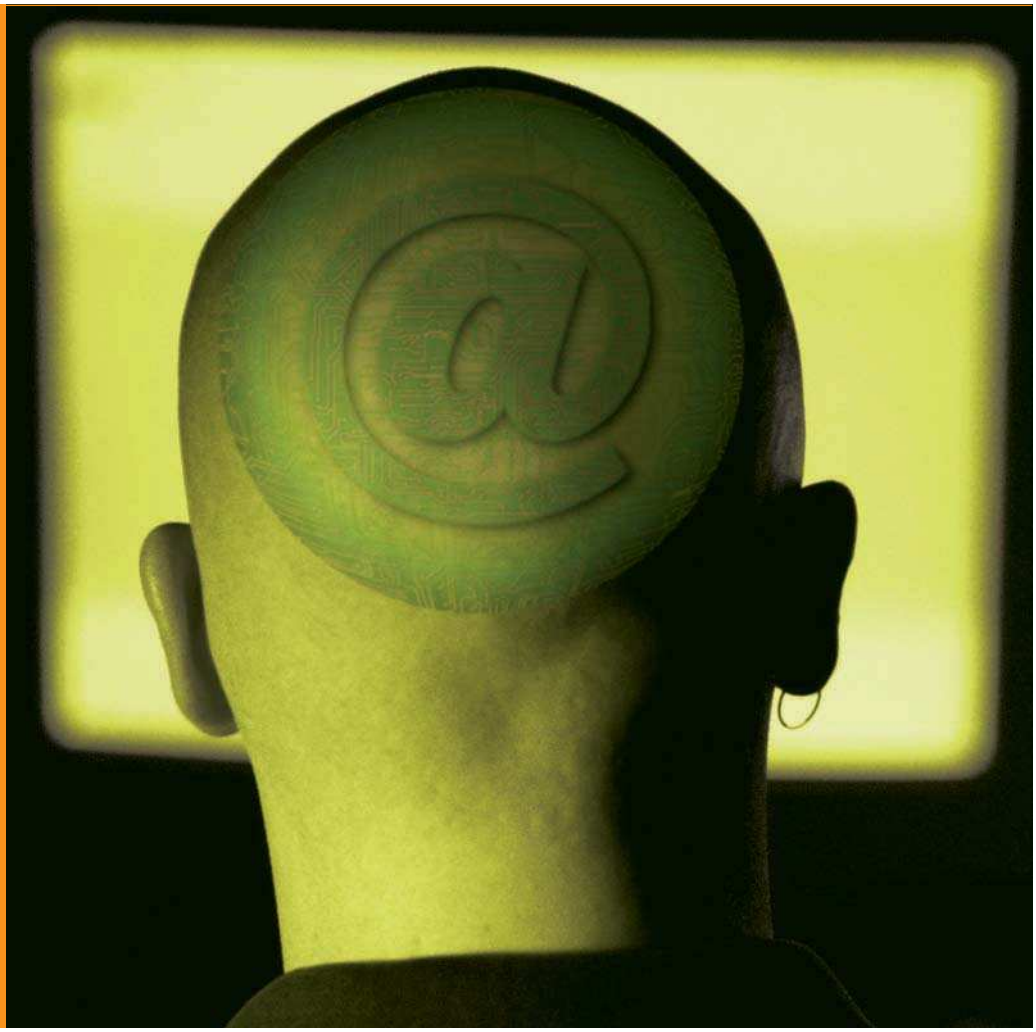


10 SUCHEN Meldet Zone Alarm den Zugriffsversuch eines unbekannten Programms, kann dessen Standort ermittelt werden.

Sicherheit unter Outlook Express

E-Mail ohne Reue

Outlook und Outlook Express sind die am meisten genutzten Programme für E-Mail-Versand und -Empfang. Gerade hier sollte das Thema Sicherheit an erster Stelle stehen.



Viele Virenpannen geschehen durch das unbedachte Öffnen von E-Mails mit Anhangdateien (auch Attachments genannt). Die Schuld den Benutzern der E-Mail-Clients alleine zuzuweisen, ist aber nicht fair, da gerade das weit verbreitete Outlook Express in den Standard-Einstellungen etliche Sicherheitslücken birgt. Durch ein paar Einstellungen und die Nutzung einiger weniger bekannter Funktionen kann man dem Problem Virus-Mail oder unerwünschte Werbe-Mails allerdings entgegenwirken. Dabei benötigen Sie noch nicht einmal zusätzliche Software.

Tipp 1: Aktuelle Versionen nutzen

SCHWIERIGKEIT: FÜR EINSTEIGER

Nach der Installation des Internet Explorers oder des Windows-Betriebssystems steht Outlook Express sofort als E-Mail-Client zur Verfügung. Sein großer Bruder Outlook bietet zwar wesentlich mehr Funktionen für interne Bürokommunikation, gleicht jedoch in den grundlegenden E-Mail-Funktionen und Einstellungen der kostenlosen E-Mail-Variante. Die hier vorgestellten Sicherungsmaßnahmen sind daher weitestgehend auf beide Programmvarianten anwendbar. Installieren Sie nach Möglichkeit immer die aktuellen Versionen von Outlook oder Outlook Express, da diese über die meisten Patches und Updates zu Sicherheitsproblemen verfügen. Informationen zu aktuellen Versionen finden Sie bei Microsoft unter www.microsoft.com/ downloads.

Tipp 2: Passwort nicht speichern

SCHWIERIGKEIT: FÜR EINSTEIGER

Grundsätzlich sollten Sie das Passwort Ihres E-Mail-Kontos unter Outlook Express oder

WAS IST?

Attachment
An eine E-Mail angehängte Datei, die aus Programmen, Archiven oder Daten bestehen kann.

Script
Befehlssequenzen wie zum Beispiel die automatische Steuerung von Word-Kommandos.

Ausführbare Datei
Startfähiges Computerprogramm, im Code des jeweiligen Prozessors geschrieben.

Logische Verknüpfung
Durch UND und ODER sowie NICHT-UND und NICHT-ODER verknüpfte Ereignisse.

Outlook nicht abspeichern. Gespeicherte Passwörter sind eine Gefahrenquelle, denn über ein solches Passwort erhalten nicht berechtigte Personen Zugriff auf alle wichtigen Daten oder Funktionen. Das Passwort eines E-Mail-Kontos lässt sich wieder entfernen, indem Sie in Outlook Express auf das Menü „Extras“ und den Eintrag „Konten“ klicken, Ihren Kontoeintrag im E-Mail-Bereich markieren, die „Eigenschaften“ anklicken und auf die Registerkarte „Server“ gehen. Entfernen Sie das Passwort (hier: „Kennwort“) und die Checkmarke für „Kennwort speichern“ und klicken Sie auf „OK“.

Tipp 3: Nachrichtigung bei Lesebestätigung

SCHWIERIGKEIT: FÜR EINSTEIGER

Achten Sie darauf, dass Ihnen die Anforderung einer Lesebestätigung angezeigt wird. In der Registerkarte „Bestätigungen“ der „Optionen“ – zu finden im Menü „Extras“ – sollte im Bereich „Versenden von Lesebestätigungen“ immer die mittlere Option „Bei Anforderung einer Lesebestätigung benachrichtigen“ aktiviert sein. Damit stellen Sie sicher, dass die Versender von Test-Mails von Onlineangeboten nur dann eine Bestätigung Ihrer E-Mail-Adresse erhalten, wenn Sie diese überprüft haben.

Tipp 4: Dateinamen korrekt anzeigen lassen

SCHWIERIGKEIT: FÜR EINSTEIGER

Sie sollten folgende Regeln bei E-Mails mit Attachment beherzigen: Installieren Sie einen guten Virenscanner, der E-Mails automatisch auf Viren prüft. Öffnen Sie niemals Attachments, deren Herkunft Sie nicht kennen. Das gilt vor allem für „heiße“ Bilder, die Ihnen „kostenlos“ zugeschickt werden. Windows stellt Ihnen nämlich ebenfalls standardmäßig eine Falle: In den „Ordneroptionen“ (Menü „Extras“ eines Ordners) unter der Registerkarte „Ansicht“ finden Sie den Eintrag „Erweiterungen der bekannten Dateitypen ausblenden“. Wenn Ihnen nun jemand einen Scriptvirus mit der Endung .vbs schickt und ihn zum Beispiel „Girls_on_Beach.JPG.vbs“ nennt, blendet Windows das „.vbs“ als bekanntes Element aus. Angezeigt wird das Attachment aber als angebliches JPEG-Bild. Wenn Sie nun darauf doppelklicken, wird anstelle des vermeintlichen Bildes ein VBS-Script ausgeführt. Sie sollten diese Option also besser abschalten, damit Dateinamen korrekt angezeigt werden. Bei Outlook sieht die Sache etwas anders aus. Die neueren Versionen zu Outlook 98 und 2000 sperren von sich aus ausführbare Dateien (Exe, Com, Bat), dagegen werden Office-Dateien ungehindert durchgelassen – was die Gefahr von Scriptviren also keinesfalls verringert. Auch hier ist es sinnvoll, die Dateinamenerweiterungen anzeigen zu lassen, um versteckte Dateifallen zu erkennen.

Tipp 5: Automatisches Senden/Empfangen aus!

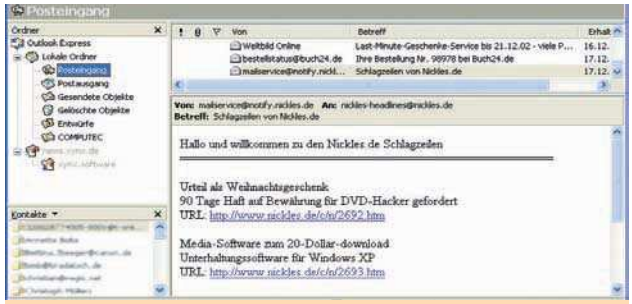
SCHWIERIGKEIT: FÜR EINSTEIGER

Ebenfalls als Vorsichtsmaßnahme lässt sich das Abschalten der automatischen Mail-Übermittlung nutzen. Dazu müssen Sie in Outlook zuerst in die „Optionen“ (Menü „Extras“) gehen. Gleich in der Registerkarte „Allgemein“ finden Sie die Checkmarke „Beim Start von Outlook Express Nachrichten senden und empfangen“. Wenn Sie diesen Eintrag deaktivieren, bleibt Outlook so lange inaktiv, bis Sie das Senden und Empfangen manuell starten. Allerdings ist diese Einstellung ebenfalls kein Garant dafür, dass nicht doch eventuell schädlicher Code mit einer Nachricht auf den Rechner gelangt.

Tipp 6: Bestimmte Absender sperren

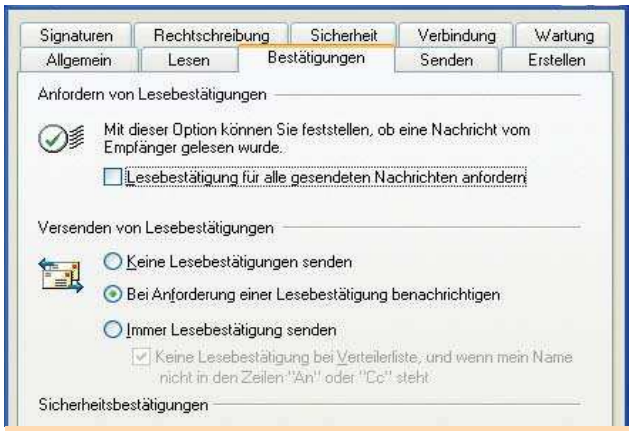
SCHWIERIGKEIT: FÜR EINSTEIGER

Wenn Sie bestimmte Nachrichten eines Absenders nicht mehr empfangen möchten, können Sie den Absender sperren. Dazu markieren Sie die gewünschte Nachricht und wählen dann im Menü „Nachrichtenregeln“ den Eintrag „Absender blockieren“. Ein Hinweisfenster zeigt Ihnen das Ergebnis des Blockade-Eintrags an. Erkennt das Blockademodul weitere Nachrichten des blockierten Absenders, kann es diese nach Rückfrage an Sie ebenfalls löschen.

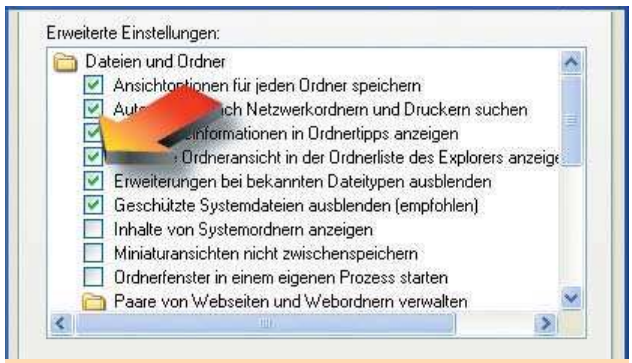


1 **OUTLOOK EXPRESS** Nicht ungefährlich: In der Standardkonfiguration werden die Inhalte von E-Mails gleich angezeigt.

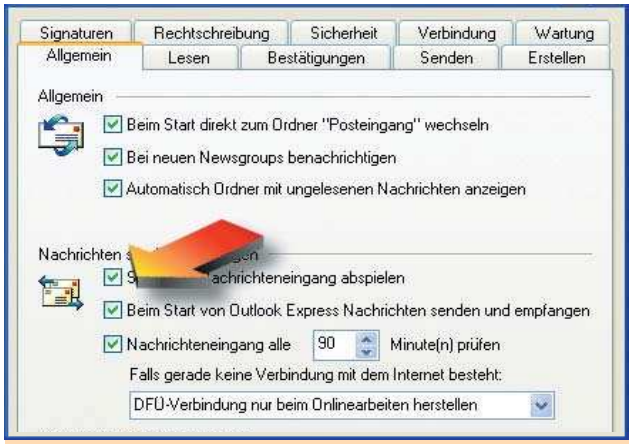
2 **PASSWORTSCHUTZ** Speichern Sie Ihr Kennwort für den E-Mail-Zugang nicht auf dem PC. Geben Sie es lieber manuell ein!



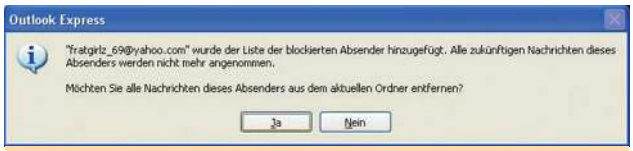
3 **NACHRICHTENBESTÄTIGUNG** Hier können Sie einstellen, dass Ihnen die Anforderung einer Lesebestätigung angezeigt wird.



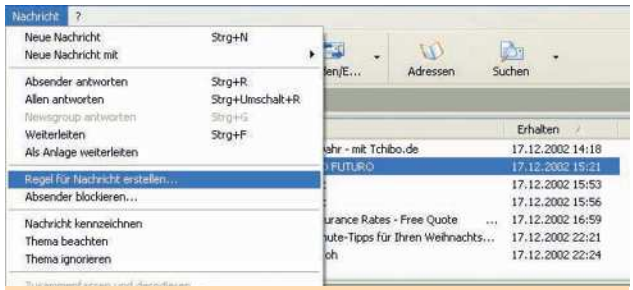
4 **DATEINAMEN** Um genau zu wissen, was sich hinter einem Attachment verbirgt, sollten Sie Dateinamen vollständig anzeigen lassen.



5 **E-MAIL-AUTOMATIK** Für ganz Vorsichtige: Wenn Sie möchten, können Sie die automatsiche Senden/Empfangen-Funktion abschalten.



6 **GEBLOCKT!** Durch Verknüpfen von Bedingungen und Aktionen können bestimmte E-Mail-Absender direkt geblockt werden.



8 **REGELWERK** Nachrichtenregeln ermöglichen es, jede ankommende E-Mail einer „Sonderbehandlung" zu unterziehen.

9 **LÖSCHEN** Sind Sie sicher, dass bestimmte Absender schädlichen E-Mail-Anhang schicken, können diese automatisch gelöscht werden.

Tipp 7: E-Mail-Regeln für Outlook Express

SCHWIERIGKEIT: FÜR FORTGESCHRITTENE

Durch die Festlegung individueller Nachrichtenregeln lassen sich E-Mails noch besser filtern. Diese Regeln unterscheiden Nachrichten in der E-Mail- und in der Newsgroup-Form durch verknüpfte Bedingungen und Aktionen. Die Regeln selbst stellen Sie entweder global für mehrere Nachrichtenkriterien oder für einzelne Nachrichten ein. Wählen Sie zum Beispiel einfach eine einzelne E-Mail per Maus aus und markieren Sie diese. Nun klicken Sie im Menü „Nachricht" auf „Regel für Nachricht erstellen ...". Daraufhin öffnet sich das Fenster für Nachrichtenregeln, in dem Sie für die einzelne Nachricht Regeln festlegen können.

Tipp 8: Nachrichten verschieben

SCHWIERIGKEIT: FÜR EINSTEIGER

Einzelne E-Mails anhand von Nachrichtenregeln zu löschen, mag gut und wichtig sein, allerdings passiert dies erst, wenn die Mail sich auf dem Rechner befindet und markiert wurde. Besser wäre es, wenn bestimmte Mails automatisch zum Beispiel in den Ordner für „gelöschte Objekte" verschoben werden könnten, ohne sie auch nur einmal mit der Maus anklicken zu müssen. Auch dabei hilft Outlook Express. Sie müssen dazu nur die entsprechende Nachrichtenregel erstellen. Ein Beispiel:

Angenommen, Sie möchten alle Nachrichten von der Domain „www.ich-schick-viren.com" direkt löschen, dann gehen Sie so vor: Zuerst klicken Sie im Menü „Extras" auf den Eintrag „Nachrichtenregeln". Im Auswahlmenü wählen Sie „E-Mail". Nachdem sich das Regelfenster geöffnet hat, sehen Sie drei Bereiche, die nacheinander zur Regelfestlegung eingesetzt werden müssen. Markieren Sie im oberen Feld („Bedingungen") das Kästchen des Eintrags „Enthält den Absender ‚Absender' ...". Im gleichen Moment ändert sich die Anzeige im dritten Abschnitt auf die ausgewählte Bedingung. Im zweiten Feld („Aktionen") markieren Sie nun das Kästchen neben dem Eintrag „In den Ordner ‚...' verschieben". Auch hier ändert sich das untere Regelfeld. Nun müssen die ausgewählten Regeln deklariert werden. Im unteren Bereich haben sich die Definitionen für die Regeleinträge in Links umgewandelt. Klicken Sie nun auf den ersten Link namens „Absender". Der Wert für „Absender" ist eine so genannte „String-Variable". Um alle Absender der oben genannten Website zu sperren, geben Sie hier den Wert „@ich-schick-viren.com" ein. Damit bleibt gewährleistet, dass alle Absender dieser Website berücksichtigt werden, solange der Absender den obigen Eintrag enthält. Nach Anklicken des Buttons „Hinzufügen" wird der Eintrag in die Liste übernommen. Wollen Sie weitere Absender bestimmter Websites auf die gleiche Weise behandeln, tragen Sie einfach weitere Namens-Variablen ein. Nun klicken Sie auf den Link beim Eintrag „Ordner" und wählen „Gelöschte Objekte". Im untersten Feld können Sie der Regel einen Namen geben. Durch Anklicken von „OK" wird die Regel übernommen und steht ab sofort zu Diensten.

Tipp 9: Löschen von Attachments

SCHWIERIGKEIT: FÜR EINSTEIGER

Über die gleichen Sicherheitsregeln lassen sich auch andere Aktionen starten, unabhängig davon, welche Regeln schon vorhanden sind. Regel 2 wird also nach Regel 1 ausgeführt, auch wenn beide Regeln gleiche Voraussetzungen haben. Das lässt eine genauere Selektion der entsprechenden Nachrichteneingänge zu. Nachdem mithilfe des letzten Tipps dafür gesorgt wurde, dass bestimmte Absender gleich im Ordner für „Gelöschte Objekte" landen, wird nun eine weitere Regel initiiert, die Nachrichten mit Attachments behandelt. Im Beispiel wird eine etwas radikalere Vorgehensweise aufgezeigt, die entsprechende Mails gleich von der Festplatte entfernt: Klicken Sie – wie im letzten Tipp beschrieben – die E-Mail-Nachrichtenregeln aus dem Menü „Extras" an. Suchen Sie im Feld „Bedingungen" den Eintrag „Nachricht hat eine An-

lage“ und im zweiten Feld „Aktionen“ den Eintrag „Nachricht löschen“ und markieren Sie die Einträge. In der Regelbeschreibung brauchen Sie diesmal nichts einzutragen, weil die Regelbestimmungen eindeutig sind. Vergeben Sie auch hier wieder einen Regelnamen und klicken Sie auf „OK“. Ab sofort werden alle Nachrichten mit Attachments rigoros aus dem Posteingang und damit von der Festplatte gelöscht, ohne dass Sie diese Mails überhaupt zu Gesicht bekommen.

Tipp 10: Regelkombinationen einrichten

SCHWIERIGKEIT: FÜR FORTGESCHRITTENE

Der eben beschriebene Vorgang hat allerdings einen entscheidenden Nachteil: E-Mails mit wichtigen Anhängen werden ebenso gelöscht wie Spam- oder Viren-Nachrichten. Outlook Express kann in seinen Regeln aber dafür sorgen, dass durch Verknüpfungen (UND/ODER) nur bestimmte Nachrichten behandelt werden. Soll eine verbesserte Selektion der durch die Regel behandelten Nachrichten erfolgen, müssen Regelbedingungen und -aktionen logisch verknüpft werden. Beispiel 1: Die Regel darf nur dann erfolgen, wenn Bedingung a UND Bedingung b eintreffen. Beispiel 2: Die Regel KANN erfolgen, wenn Bedingung a ODER Bedingung b eintrifft. Eine mögliche Regel für eine UND-Verknüpfung wäre: „Enthält den Absender ‚Absender' in der ‚Von'-Zeile“ und „Enthält den Text ‚Text' in der Betreffzeile“. Treten beide Bedingungen ein, wird die Nachricht zum Beispiel in den Ordner „Gelöschte Objekte“ verschoben. Tritt nur eine Bedingung ein, bleibt die Nachricht im E-Mail-Eingang. Wird über den Aktionslink anstelle des UND ein ODER gewählt, braucht nur eine der Bedingungen einzutreffen, um die Nachricht zu verschieben. Durch Kombination mehrerer Regeln mit Anwendung auf eine Nachrichtenart kann man so genau bestimmen, wann eine E-Mail gelöscht, verschoben oder im Ordner belassen werden soll. Klären Sie außerdem im Vorfeld ab, von wem Sie Attachment-Mails erhalten dürfen!

Tipp 11: Wortliste einrichten

SCHWIERIGKEIT: FÜR FORTGESCHRITTENE

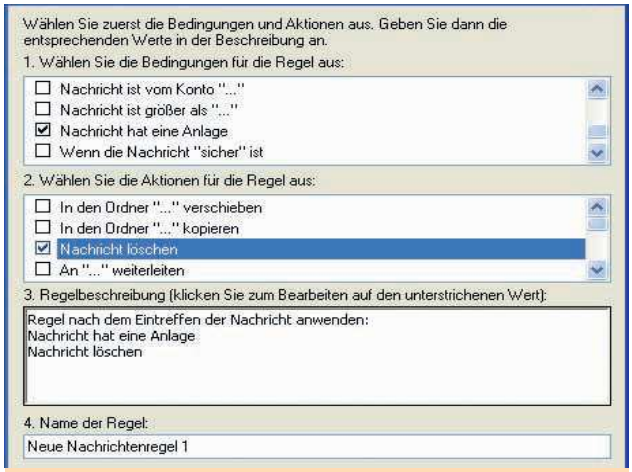
Über das Regelwerk von Outlook Express können Sie sogar einen kleinen Spam-Filter einrichten: Die meisten unerwünschten Werbemails basieren auf immer dem gleichen Wortschatz. „Sex“, „Porn“, „Money“, „Free“ sind immer wiederkehrende Stichwörter für Spam aus dem englischsprachigen Raum. Durch Anwahl der Bedingung „Enthält den Text ‚Text' im Nachrichtentext“ und der Aktion „Löschen“ können Sie solche unerwünschten E-Mails gleich aus dem Outlook-Bereich filtern. Dazu geben Sie einfach in der Wortliste alle bekannten Wörter ein und verknüpfen sie mit der gewünschten Aktion. Der „Button“ Optionen öffnet ein Untermenü, in dem Sie die Wörter sogar noch mit weiteren Unterbedingungen („nicht enthalten/enthalten“ oder „entspricht/entspricht teilweise“) verknüpfen können.

Fazit: Der Aufwand lohnt sich!

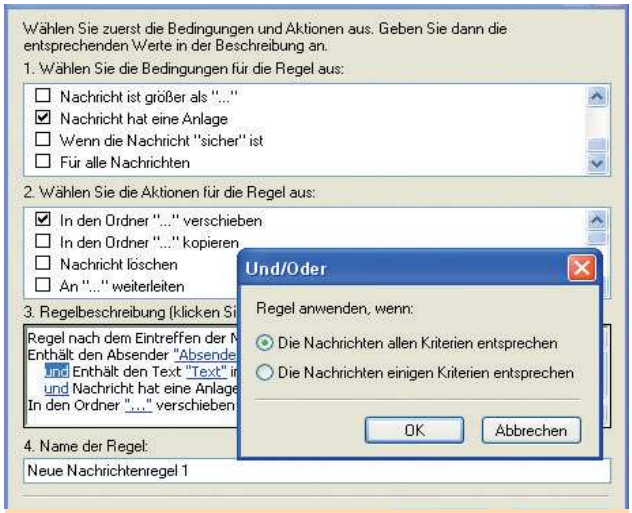
SCHWIERIGKEIT: FÜR EINSTEIGER

Microsoft hat mit Outlook und Outlook Express zwei recht komfortable Kommunikationsprogramme geschaffen – bei der Sicherheit jedoch sind beide Windows-Produkte nicht gerade erste Wahl. Die hier beschriebenen Filterregeln helfen zumindest ansatzweise dabei, den E-Mail-Client vor Dateien mit gefährlichen Inhalten zu schützen. Doch eines muss klar sein: Ohne ein aktuelles und update-fähiges Antiviren-Programm sind die installierten Filterregeln nur ein winziger Bruchteil von dem, was an Sicherheit wirklich notwendig ist. Und Outlook und Outlook Express bleiben ohne spezielle Firewall, die anders als die in Windows XP integrierte nicht nur eingehende, sondern auch ausgehende Kommunikation überwacht, dank der immer wieder neu entdeckten Sicherheitslöcher Lieblingsziele von Angreifern. Die wichtigste Regel muss der Benutzer allerdings selbst beherzigen: Nicht alles öffnen, was E-Mails als Attachment mitbringen.

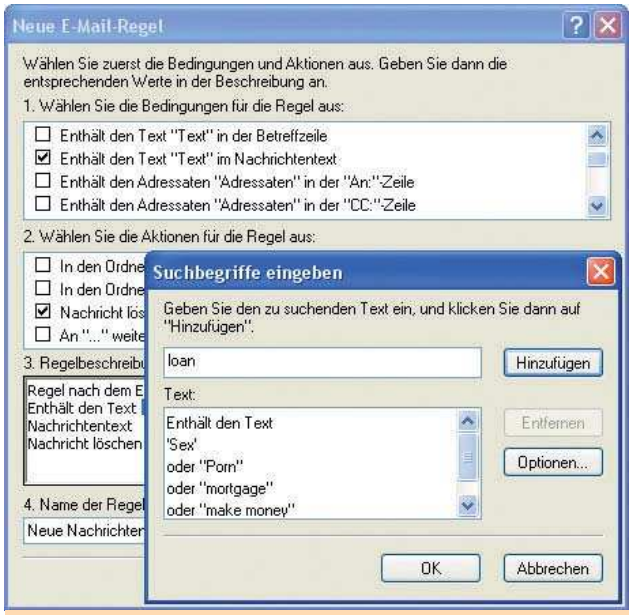
JÜRGEN BORNGIESSER



10 **VERKNÜPFEN** Das Verknüpfen von Nachrichtenregeln in Outlook Express erlaubt es, E-Mails noch genauer zu selektieren.



10 **REGEL-KOMBI** Durch Kombination mehrerer Regeln können Sie auch bestimmen, wie Outlook gewisse Mails behandeln soll.



11 **SPAMFILTER** Verknüpft man typische Begriffe aus Werbe-E-Mails miteinander, lässt sich ein wirkungsvoller Spamfilter einrichten.

Hackerangriffe erkennen und abwehren

Keine Chance für Hacker

Hacker-Angriffe auf fremde Systeme sind heutzutage fast schon zu einer Art Sport unter gewissenlosen Computerfreaks geworden. Auch Ihr PC könnte das nächste Ziel von Hackern werden. In diesem Praxis-Artikel lesen Sie, wie Sie sich erfolgreich zur Wehr setzen.

Das „Hacking" ist beinahe so alt wie der Computer selbst. Demnach stammt auch das Wort „Hacker" aus den Anfangstagen des Computers. Es bezeichnete ursprünglich besonders fähige Programmierer, die sich gerne mit sehr komplexen Problemen beschäftigten. Im Grunde war dies also eine positive Bezeichnung – doch Qualität und Sinn dieses Titels änderte sich im Laufe der Zeit. Als es bei – meist jugendlichen – Computerfreaks in wurde, zum Vergnügen in fremde Computersysteme einzubrechen, fiel in diesem Zusammenhang immer wieder der Begriff „Hacking". Die ursprünglichen, aufrichtigen Hacker missbilligten dieses Treiben allerdings und titulierten solche Personen spöttisch als „Cracker". Beide Bezeichnungen sind heute gleichermaßen negativ behaftet und stehen synonym für alle Formen der Computerkriminalität, angefangen vom Einbruch in Computersysteme bis hin zum Umgehen von Kopierschutzmechanismen von Software. Während früher fast ausschließlich staatliche Einrichtungen und große Konzerne zu den Opfern von Hacker-Angriffen gehörten, so wird mittlerweile auch der private PC immer öfter zur Zielscheibe der Hacker.

Tipp 1: IP-Adresse des Hackers ermitteln

SCHWIERIGKEIT: FÜR FORTGESCHRITTENE

In unserem Praxis-Artikel „Schützen Sie Ihre Identität" haben Sie bereits gelernt, wie Sie Ihre eigene IP-Adresse herausfinden. Stellen Sie sich vor, Sie werden von einem Hacker angegriffen – wäre es da nicht sinnvoll, auch seine IP-Adresse zu kennen? Am einfachsten gelingt dies mithilfe der kostenlosen Firewall Zone Alarm (siehe hierzu auch „Workshop mit Zone Alarm" in diesem Heft). Um die IP-Adresse von potenziellen Angreifern zu ermitteln, gehen Sie wie folgt vor: Öffnen Sie Zone Alarm zunächst mit einem Doppelklick auf das Symbol in der Windows-Traybar unten rechts. Wechseln Sie nun auf die Registerkarte „Alerts &Logs". Im daraufhin erscheinenden Dialog „Internet Alerts" setzen Sie bitte bei der Option „Alert Events Shown" ein Häkchen. Jedes Mal, wenn jetzt ein Hacker versucht, in Ihr System einzudringen, erhalten Sie eine Warnmeldung, in der Ihnen unter anderem die IP-Adresse des Angreifers mitge-

WAS IST?

Hacker
Allgemeine Bezeichnung für Computerfreaks, die versuchen, in fremde Systeme einzubrechen

Spam
Täglich eingehende, unerwünschte Werbe-Mails mit oft zweifelhafter Herkunft

IP-Adresse
IP steht für Internet Protocoll. Jedem Rechner im Netz wird eine Kenn-Nummer zugewiesen.

Visual Route
Programm, mit dem der Weg eines Datenpaketes durchs Netz zurückverfolgt werden kann

und Spammer!

teilt wird. Um auch wirklich keinen Alarm zu übersehen, sollten Sie zudem die Funktion „Log alerts to a text file“ aktivieren, da auf diese Weise alle Meldungen in einem Textdokument protokolliert werden.

Tipp 2: Spur des Hackers zurückverfolgen

SCHWIERIGKEIT: FÜR FORTGESCHRITTENE

Wenn Ihnen Ihre Firewall meldet, dass Sie gerade von außen angegriffen werden, gilt es schnell zu handeln. Am besten können Sie nämlich gegen einen Hacker vorgehen, wenn Sie möglichst viele Daten über ihn haben. Nutzen Sie die Zeit, während Sie und der Hacker noch online sind, und sammeln Sie erste Daten. Der Standort des Hackers ist schließlich nicht ganz uninteressant: Es könnte ja sein, dass es sich dabei um Ihren Nachbarn handelt. Rufen Sie als Erstes die Eingabeaufforderung über „Start“ – „Programme“ – „Zubehör“ auf. Geben Sie anschließend über die Tastatur Folgendes ein: „tracert <IP-Adresse>“. Hiermit aktivieren Sie ein kleines Programm namens Trace-Route, das den rückläufigen Pfad zu der angegebenen Adresse ermittelt und Ihnen dabei alle Netzwerkrechner anzeigt, über die die Verbindung von Ihnen zur genannten IP-Adresse hergestellt wird. Anhand der Rechnernamen lässt sich manchmal schon ungefähr sagen, wo der Zielrechner steht und in welchen Städten die Zwischenstationen installiert sind, wobei diese allerdings mit dem Angriff nichts zu tun haben, da sie nur die Datenpakete transportieren. Tipp: Falls Ihnen Trace-Route zu unübersichtlich ist, empfehlen wir Ihnen das Programm Visual Route, das Sie als Demoversion unter www.visualware.com/download/index.html herunterladen können.

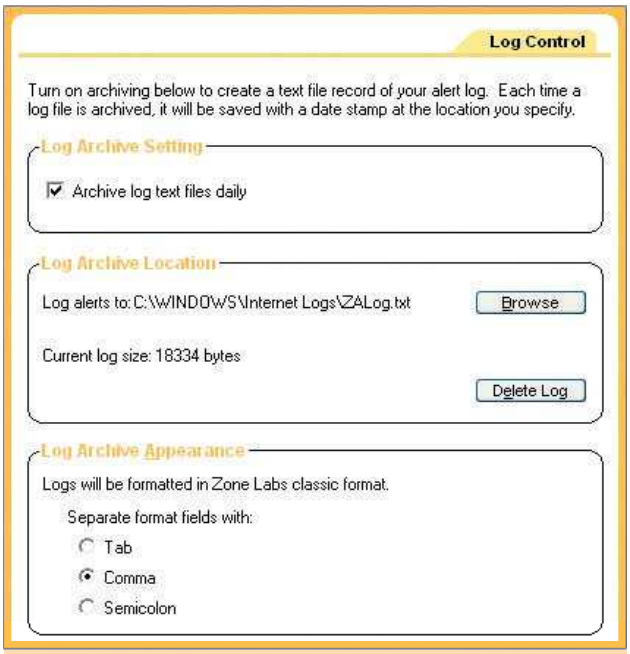
Nach Installation des Programms geben Sie bei „Address“ einfach die gesuchte IP-Adresse oder einen Domainnamen ein und starten die Suche mit „Enter“. Auch hier erhalten Sie Informationen darüber, über welche Rechner eine Verbindung zum Zielsystem hergestellt werden kann. In der Weltkarte werden die Standorte der Stationen eingezeichnet und durch eine Line verbunden. Zusätzlich können Sie noch per Mausklick in die Karte hinein- und hinauszoomen.

Tipp 3: Ermitteln, wem die IP-Adresse gehört

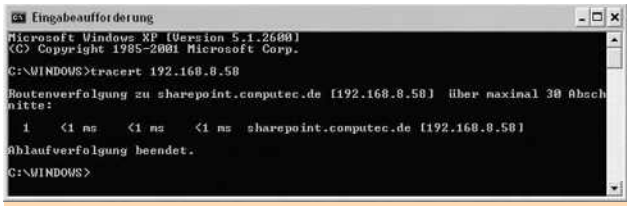
SCHWIERIGKEIT: FÜR PROFIS

Nachdem Sie die IP-Adresse des Hackers herausgefunden haben, können Sie sich jetzt daranmachen, noch mehr Informationen über den Hacker zu sammeln: Woher kommt der Hacker und über welchen Provider geht er ins Netz? Speziell letztere Information ist wichtig, denn Provider haben etwas gegen solche Leute und werden Ihnen daher bestimmt im Kampf gegen den Angreifer helfen. Doch als Erstes brauchen Sie die Hilfe der Website www.arin.net der Organisation American Registry for Internet Numbers (ARIN). Geben Sie auf der Homepage rechts oben im Feld „Search Whois“ (englisch für „wer ist“) die IP-Adresse desjenigen ein, der Sie ange-

1 MELEDEPFLICHT Zone Alarm meldet auf Wunsch jeden Angriff auf Ihren PC – nebst der IP-Adresse des Störenfrieds.



1 PROTOKOLL Aktivieren Sie die Option „Archive log text files dalay", protokolliert Zone Alarm jeden Angriff in einem Textdokument.



2 SPURENSUCHER Über den Befehl „tracert" wird ein Tool aktiviert, dass eine IP-Adresse bis zu ihrem Ausgangsrechner zurückverfolgt.

2 VISUAL ROUTE Mittels einer Weltkarte zeigt dieses Tool den Weg einer IP-Adresse über die einzelnen Stationen bis zum Zielrechner.

griffen hat, und starten Sie die Suche. Meistens bekommen Sie dann keine direkte Auskunft, sondern Ihnen wird die Registrierungsstelle mitgeteilt, die für diese IP-Adresse zuständig ist. Ist dies der Fall, klicken Sie auf den Link bei „Coordinator". Neben einigen Informationen über den zuständigen Koordinator erscheint auch der Link zu dessen Website. Bei der entsprechenden Koordinierungsstelle werden Sie wiederum eine Whois-Datenbank finden, wo Sie die gesuchte IP-Adresse erneut eingeben können. Nun erhalten Sie endlich die gewünschte Information und wissen, welchen Anschluss der Hacker benutzt. Wenn Sie Glück haben, ist sogar eine Kontaktadresse angegeben (mit „remarks" gekennzeichnet), bei der Sie sich beschweren können.

Tipp 4: Spammern das Handwerk legen

SCHWIERIGKEIT: FÜR FORTGESCHRITTENE

Haben Sie es mit solch ungeliebten Zeitgenossen wie Spammern zu tun, ärgern Sie sich bestimmt täglich über die eingehende E-Mail-Flut. Doch auf den entsprechenden Websites, auf die die Spam-Mails hinweisen, sucht man meist vergeblich nach einer Kontaktadresse, bei der man sich beschweren kann. Was viele nicht wissen: Es gibt eine offizielle Stelle unter www.nic.com, bei der Sie Auskünfte über den Betreiber einer Internetseite einholen können. Jede Seite muss nämlich bei einer Registrierungsstelle angemeldet sein. Neben Informationen über die Webdomain finden Sie hier in vielen Fällen auch Name, E-Mail-Adresse, Anschrift sowie Telefon- und Faxnummer.

Eine weitere Möglichkeit, um den Spammer ins Visier zu nehmen, ist, herauszufinden, welche E-Mail-Software er benutzt. Sehen Sie sich den Kopf der Spam-Mail genauer an. Hier gibt es meist einen Eintrag mit dem Vortext „X-Mail". Dahinter kann vom E-Mail-Programm ein beliebiger Text eingetragen werden. Benutzt der Spammer beispielsweise AOL als E-Mail-Client, würde der entsprechende Eintrag folgendermaßen lauten: „X-Mailer: AOL 6.0 for Windows US sub 10xxx". Mit dieser Information können Sie den Spammer also als AOL-Kunden entlarven. Da kein seriöser Provider Spammer toleriert, könnte es erfolgversprechend sein, sich an den Kundenservice von AOL zu wenden, um den Spammer dann weiterzuverfolgen.

Tipp 5: Nur zu legalen Mitteln greifen!

SCHWIERIGKEIT: FÜR EINSTEIGER

Wenn Sie alle Informationen über den Angreifer zusammenhaben, wird es Zeit, etwas gegen ihn zu unternehmen. Machen Sie dabei aber unbedingt von legalen Mitteln Gebrauch und versuchen Sie keinesfalls, auf Hacker-Art einen Gegenangriff zu starten. Es gibt eine Reihe von Möglichkeiten, mit denen Sie dazu beitragen können, Hacker aus dem Verkehr zu ziehen und sich selbst und andere in Zukunft vor derartigen Angriffen zu schützen.

Tipp 6: Den Hacker auffliegen lassen

SCHWIERIGKEIT: FÜR EINSTEIGER

Hacker und Spammer gehören nicht gerade zu den Lieblingskunden von Providern, weshalb Sie sich als Erstes mit der Information an den entsprechenden Systembetreiber wenden sollten, dass jemand versucht hat, von seinem System aus einen Hackversuch zu starten. Die Administratoren werden dann mit dem Hacker Verbindung aufnehmen und ihn verwarnen oder gleich ausschließen. Schließlich verbraucht er Rechenzeit, Bandbreite und schädigt außerdem den Ruf des Betreibers.

Tipp 7: Informieren Sie die Systembetreuer

SCHWIERIGKEIT: FÜR EINSTEIGER

In den vorangegangenen Schritten haben wir Ihnen gezeigt, wie Sie herausfinden, von welchem Rechner aus der Angriff gestartet wurde. Mit diesen Informationen sollten Sie sich zuerst an den jeweiligen Systembetreuer wenden. Wenn Sie den Systembetreuer nicht sofort ausfindig machen können, probieren Sie einfach diese E-Mail-Adressen aus: abuse@name-der-domain, admin@name-der-domain oder root@name-der-domain. In Ihrer Mail an den Betreiber sollten Sie unbedingt folgende Informatio-

nen anführen: Wann und auf welche Art ist Ihr Rechner angegriffen worden (Tag, sekundengenaue Uhrzeit sowie Protokoll, Portnummern und alles andere, was Sie beobachtet haben)? Einen Teil dieser Informationen finden Sie in den Log-Dateien Ihrer Firewall. Alternativ dazu notieren Sie sich die Alarmmeldungen, die von der Firewall am Bildschirm angezeigt werden.

Tipp 8: Strafrechtliche Mittel einleiten

SCHWIERIGKEIT: FÜR EINSTEIGER

Wenn Sie Opfer eines Hacker-Angriffs geworden sind und Schaden davongetragen haben, sollten Sie darüber nachdenken, den Übeltäter anzuzeigen. Es ist dabei völlig unerheblich, ob Ihr Rechner dabei tatsächlich Schaden genommen hat, „nur" Daten gestohlen wurden oder ob Sie durch den Hacker-Angriff zusätzliche Arbeitszeit aufbringen mussten – beispielsweise weil das System komplett neu aufgesetzt werden musste.

Erfolgversprechend ist eine Anzeige allerdings nur, wenn Sie möglichst viele Beweise vorbringen können. Daher gilt: Dokumentieren Sie so genau wie möglich den kompletten Angriff. Fertigen Sie Screenshots an und sichern Sie alle verfügbaren Informationen wie zum Beispiel Log-Dateien. Ist es Ihnen gelungen, mithilfe oben genannter Tipps den Hacker zu identifizieren, sollten Sie natürlich auch diese Informationen aufheben.

Sollten Sie vorhaben, den Hacker anzuzeigen, bedenken Sie aber bitte, dass eine Straf- oder Zivilanzeige mit großem Aufwand verbunden ist, der in einem gesunden Verhältnis zum tatsächlich angerichteten Schaden stehen sollte. Professionelle Hacker, die in der Lage sind, wirklich großen Schaden anzurichten, richten ihre Attacken meist gegen große Konzerne oder staatliche Einrichtungen und nicht gegen Privatpersonen. Problematisch wird es, wenn Hacker und besonders Spammer außerhalb der EU tätig sind. Selbst innerhalb der EU gibt es noch keine einheitlichen Richtlinien, wie mit Spam-Mails, Kettenbriefen und dergleichen zu verfahren ist. Informationen zu einschlägigen Gerichtsurteilen zu diesem Thema finden Sie beispielsweise unter der Adresse www.jurpc.de/aufsatz/20000047.htm. Wenn der Hacker außerhalb der EU sitzt, werden Sie kaum eine Chance haben, ein Gerichtsverfahren gegen ihn anzustrengen, da es immer noch umstritten ist, welches nationale Recht nun gilt: das im Land des Opfers oder das im Land des Angreifers. Die damit verbundenen Kosten lassen eine solche Aktion oft schon im Vorfeld scheitern.

Tipp 9: Sichern Sie Ihren Browser ab!

SCHWIERIGKEIT: FÜR EINSTEIGER

Bei all den Gefahren, die wir Ihnen bisher geschildert haben, und dem zusätzlichen Aufwand, den diese nach sich ziehen, soll jedoch der Spaß am Umgang mit PC und Internet nicht verloren gehen. Die Vorsorge spielt dabei eine entscheidende Rolle, denn je mehr Sicherheitsvorkehrungen Sie im Vorfeld getroffen haben, umso beruhigter können Sie sich im World Wide Web bewegen. Wie bereits schon an etlichen Stellen in diesem Heft besprochen, gehören die richtigen Sicherheitseinstellungen im Browser zu den wichtigsten Schutzmaßnahmen. Da speziell der Internet Explorer von Microsoft in seinen Standardeinstellungen ein großes Sicherheitsrisiko darstellt, können Sie alternativ gleich zu einem anderen Browser wie Mozilla (www.mozilla.org) wechseln, der als äußerst sicher und leistungsfähig gilt. Dies ist aber nicht unbedingt nötig, da sich unter der Haube des Internet Explorers viele leicht zugängliche Konfigurationsmöglichkeiten verbergen, mit denen Sie fast alle Sicherheitslücken schließen können.

Tipp 10: Zonenmodell im Internet Explorer

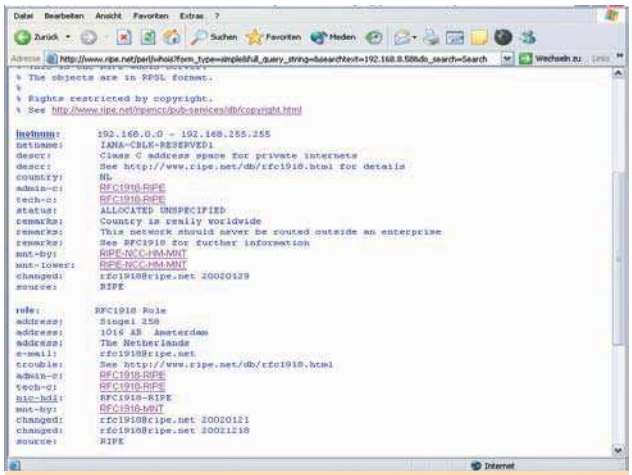
SCHWIERIGKEIT: FÜR EINSTEIGER

Auf eine Besonderheit im Internet Explorer wollen wir kurz näher eingehen: das so genannte Zonenmodell. Der Browser unterscheidet bei der Anzeige von Webseiten vier Zonen, die jeweils unterschiedliche Sicher-

3 WHO IS? Über die Website www.arin.net können Sie über eine Suchfunktion herausfinden, zu wem eine bestimmte IP-Adresse gehört.

3 REGISTRIERUNGSSTELLE Falls Sie über ARIN keine direkte Auskunft erhalten, finden Sie einen Link zum entsprechenden Koordinator.

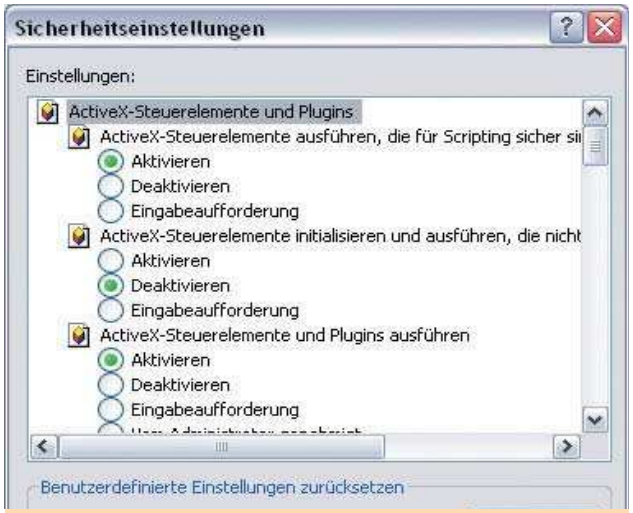
3 KOORDINATOR Beim Koordinator bekommen Sie durch erneutes Eingeben der IP-Adresse die gewünschten Infos über den Besitzer.



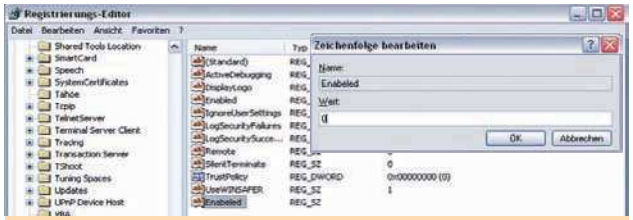
3 INFOS NUTZEN! Neben Informationen zum möglichen Standort eines Hackers finden Sie hier manchmal auch eine Kontakt-Adresse.

8 RECHTLICHES Auf der Seite www.jurpc.de finden Sie Informationen zu Urteilen bezüglich Spam, Hacking, Kettenbriefen und dergleichen.

10 ZONENMODELL Für jede der vier Zonen lassen sich im Internet Explorer verschiedene Sicherheitseinstellungen vornehmen.



10 VERTRAUENSWÜRDIGE SITES In dieser Zone legen Sie fest, welchen Seiten Sie mehr Privilegien zubilligen möchten.



11 REGEDIT Legen Sie hier eine neue Zeichenfolge mit dem Namen „Enabled" und dem Wert „0" an, um Active Scripting zu verhindern.

heitseinstellungen haben können. Zu diesen Zonen gehört als Erstes „Internet", womit alle Webseiten gemeint sind, die nicht in den anderen Zonen liegen beziehungsweise diesen nicht zugerechnet werden. Die nächste Zone ist „Lokales Intranet": Dazu gehören Webseiten aus Ihrem persönlichen oder geschäftlichen Intranet. Über den Button „Sites" können Sie einstellen, welche verschiedenen Webseitenherkünfte noch zur Intranetzone gezählt werden sollen.

Eine sehr wichtige Zone ist „Vertrauenswürdige Sites". Hier haben Sie die Möglichkeit, einzelne Seiten – ebenfalls über die Schaltfläche „Sites" – als vertrauenswürdige Seiten in eine Liste aufzunehmen. Tragen Sie die Seiten ein, denen Sie mehr Privilegien zubilligen, und klicken Sie anschließend auf „Hinzufügen". Wenn Sie die Option „Für Sites dieser Zone ist eine Serverprüfung (https) erforderlich" aktivieren, lassen sich hier nur Websites eintragen, die per SSL verschlüsselt werden und den entsprechenden https-Vorspann benutzen. In der letzten Zone finden Sie „Eingeschränkte Sites". Hier gehören alle Seiten hin, denen Sie nicht vertrauen und für die entsprechend hohe Sicherheitsbestimmungen gelten sollen. Auch hier weisen Sie die Seiten mit der Schaltfläche „Sites" zu.

Tipp 11: Scripting Host verhindern

SCHWIERIGKEIT: FÜR PROFIS

Neben den Browser-Einstellungen sollten Sie noch Ihr Betriebssystem gegen Hackerangriffe absichern. Zwar bietet eine Firewall bereits guten Schutz gegen Angriffe, doch die von Microsoft stammenden Programmiersprachen J-Script und VB-Script bieten Hackern eine Angriffsfläche, die – um ganz sicherzugehen – noch mehr Sicherheitsvorkehrungen nötig machen. Mit J-Script und VB-Script werden Websites mit dynamischen Inhalten entwickelt und sie dienen auch dazu, bestimmte Aufgaben auf einem lokalen Rechner zu automatisieren. Letzteres soll für den Benutzer eigentlich eine Hilfe sein, da mit diesen leicht zu erlernenden Sprachen Programme erstellt werden können, die immer wiederkehrende Aktionen automatisch ablaufen lassen.

Hacker missbrauchen diese sinnvolle Funktion, um auf fremden PCs bestimmte Aktionen auszuführen. Da das Script-Programm nach seinem Start Administrator-Rechte bekommt, gibt es eigentlich nichts, was es auf dem System nicht tun kann: Viren per E-Mail versenden, die Festplatte formatieren und so weiter. Um es nicht so weit kommen zu lassen, führen Sie unter Windows (in unserem Fall Windows XP) folgende Schritte durch:

Starten Sie den Registrierungseditor durch Eingabe von „regedit" im Fenster „Start/Ausführen". Öffnen Sie anschließend den Schlüssel „HKEY_LOCAL_MACHINE" – „SOFTWARE" – „Microsoft" – „Windows Script Host" – „Settings". Mit „Bearbeiten" – „Neu" – „Zeichenfolge" legen Sie jetzt eine neue Zeichenfolge an. Danach benennen Sie die neue Zeichenfolge in „Enabled" um und bestätigen mit „Enter". Drücken Sie erneut „Enter" (der Name muss noch markiert sein) und es erscheint ein Fenster, in dem Sie einen Zahlenwert eingeben müssen. Tragen Sie „0" ein. Anschließend beenden Sie den Registrierungseditor. Ab jetzt kann sich kein Virus mehr per Active Scripting in Ihrem System verbreiten.

Fazit: Wie auch immer sich ein Hacker-Angriff auf Ihren PC bemerkbar macht. Ob Sie materiellen oder immateriellen Schaden erleiden oder einfach nur den Versuch eines Angriffs registrieren: Hacking ist kein Kavaliersdelikt! In diesem Zusammenhang sei noch mal darauf hingewiesen, dass auch Gegenangriffe – und sei es nur zur Verteidigung – strafbar sind. Setzen Sie die hier vorgestellten legalen Mittel ein und sorgen Sie vor! Eine zuverlässige Firewall, ein aktueller Virenscanner und sichere Browser-Einstellungen dämmen die Gefahr aber nämlich im Vorfeld ein.

FRANK NEUPERT

ideenhaus muc

WWW.PCGAMESHARDWARE.DE

NOCH BILLIGER FRISIEREN!

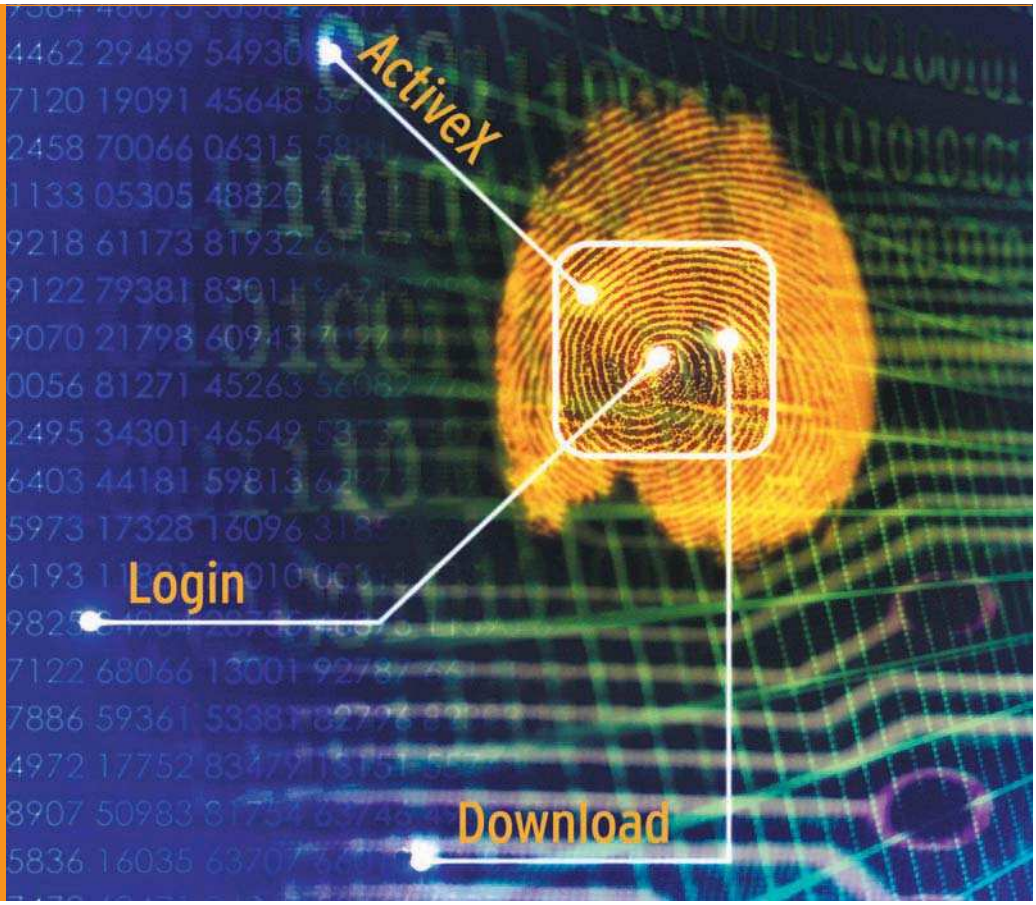
DIE OPTIMALE TYPBERATUNG FÜR GÜNSTIGES PC-TUNING

- JEDE MENGE CLEVERE TIPPS UND NEWS FÜR BESSERES PC-ENTERTAINMENT.
- JEDES HEFT MIT CD-ROM INKL. GRATIS-TOOLS & CO.
- JEDEN MONAT FÜR SCHLAPPE 3,99 EURO.

3 Browser im Praxistest

Sicherheit beim Browsen

Die größte Schwachstelle für die Sicherheit eines Windows-PCs ist der Internetzugang. Und daran ist vor allem der Browser schuld, da er sozusagen das Tor zum eigenen Computer weit öffnet.



Seit es Browser gibt, sind auch immer wieder Versuche zu verzeichnen, über diese Zugang zu lokalen Rechnern zu erhalten, um nicht-öffentliche Daten auszuspionieren oder – schlimmer noch – den lokalen PC zu schädigen. Während sich in der Anfangszeit das „Hacken" eher darauf spezialisierte, sich durch Angriffe auf kommerzielle Rechnersysteme – zum Beispiel bei Online-Banken oder Mehrwertdiensten – einen Vorteil zu verschaffen, gehört mittlerweile verstärkt der private Rechner zum beliebten Ziel für Hacker-Angriffe. Wer im Internet danach sucht, findet jede Menge Hacker-Tools für den „Hausgebrauch": Trojaner, Nuke-Programme, BruteForce-Tools, mit denen man durch automatisches Senden von zufällig oder durch ausgeklügelte Algorithmen erzeugten Passwort-Sequenzen Zugänge „knackt" und vieles mehr. Viele dieser Tools finden einen einfachen Zugang zum Rechner des Internet-Surfers: Durch den Browser. Dessen Sicherheitsmechanismen entscheiden darüber, wie sicher Ihre Daten vor dem unberechtigten Zugriff Dritter sind.

Alternativen sind möglich

SCHWIERIGKEIT: FÜR EINSTEIGER

Der meistgenutzte Browser ist der Internet Explorer von Microsoft. Nachdem Microsoft dafür sorgen musste, dass Windows-Betriebssystem und Browser nicht mehr „verzahnt" arbeiten, sind alternative Browsersysteme für den Einsatz unter Windows interessant geworden. Neben dem Internet Explorer haben sich inzwischen drei andere Browser etabliert, von denen wir die zwei weniger verbreiteten mal im Bereich Sicherheit dem Internet Explorer gegenüber stellen möchten: „Opera" und „Mozilla". Auf die Vorstellung des Netscape-Browsers soll hier verzichtet werden, er entspricht bis auf seine eigenen Erweiterungen eigentlich dem Mozilla-System, so dass dieses als „Urvater" herhalten kann. Und Opera ist als Alternative zu den beiden „Großen" schon immer im Gespräch gewesen. Unser Test soll daher zeigen, wo sich die Schwachstellen befinden, aber auch, wo die Sicherheitsmaßnahmen der drei Browsersysteme zu finden sind und wie diese am besten genutzt werden. JÜRGEN BORNGIESSER

WAS IST?

Hacker-Tools
Sammelbegriff für spezielle Programme zum Hacken, Passwort-Knacken oder Stören von Internetdiensten infolge ihres Einsatzes

Brute Force
Hacker-Tool zum Ermitteln von Passwörtern durch Generieren von Code-Sequenzen und Übermitteln an die Passworteingabe

Nuke-Programms
Tools zum „Abschießen" von Systemen. Dabei wird durch teilweise unsinnige Systembefehle ein Absturz über das Netzwerk verursacht.

Vorsicht beim IExplorer!

Microsofts Internet Explorer wird genutzt, weil er Windows kostenlos beiliegt. Die Sicherheitseinstellungen des Browsers würden aber eher zur Alternative raten – sofern man nichts daran ändert.

Der Internet Explorer ist gerade in der aktuellen Version 6 ein überaus komfortables und leicht zu bedienendes Programm. Aber gerade diese Schlichtheit ist das Problem – vielen Internetnutzern ist nicht bekannt, dass ihr Explorer Daten sammelt und speichert, die genaue Informationen über besuchte Webseiten oder genutzte Internetdienste enthalten und somit ein ausführliches User-Profiling ermöglichen.

Tipp 1: Cache leeren

SCHWIERIGKEIT: FÜR EINSTEIGER

Die wichtigste Maßnahme für minimalen Schutz ist das regelmäßige Löschen des Caches. Der Explorer legt im Ordner „Temporary Internet Files“ alles ab, was er auf Webseiten findet, damit bei einem neuerlichen Besuch nicht geänderte Dateien sofort angezeigt werden können. Die im Verzeichnis „Systemeinstellungen“ befindlichen „Internetoptionen“ enthalten mehrere wichtige Einträge zum Löschen aller Cache-Inhalte, die von Webseiten mit entsprechenden Programmen ausgelesen und zurückverfolgt werden können. Dazu gehören das separate Löschen von „Cookies“ sowie das Löschen aller enthaltenen Text-, HTML- oder Bilddaten.

Tipp 2: ActiveX-Kontrollen einschränken

SCHWIERIGKEIT: FÜR EINSTEIGER

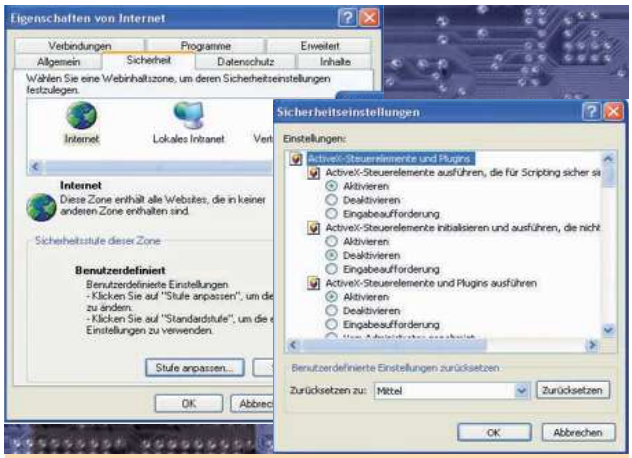
Das schwerwiegendste Problem beim Internet Explorer ist die standardmäßig eingestellte Sicherheitsstufe. Ebenfalls in den „Internetoptionen“ unter der Registerkarte „Sicherheit“ findet sich ein Button mit der Aufschrift „Stufe anpassen“. Über diesen ist es möglich, für die entsprechende Netzwerkverbindung (LAN oder DFÜ) die Einstellungen anzupassen. So ist standardmäßig zum Beispiel das Ausführen von ActiveX-Kontrollelementen auf Webseiten erlaubt, was zu schweren Problemen führen kann. ActiveX-Kontrollen ermöglichen zum Beispiel gezieltes „Lenken“ des Browsers, automatisches Starten von externen Programmen oder neuen Fenstern, automatisches Ausführen von Scripten oder zusätzlichen Plug-Ins (zum Beispiel „Dialer“).

Tipp 3: AutoVervollständigen regulieren

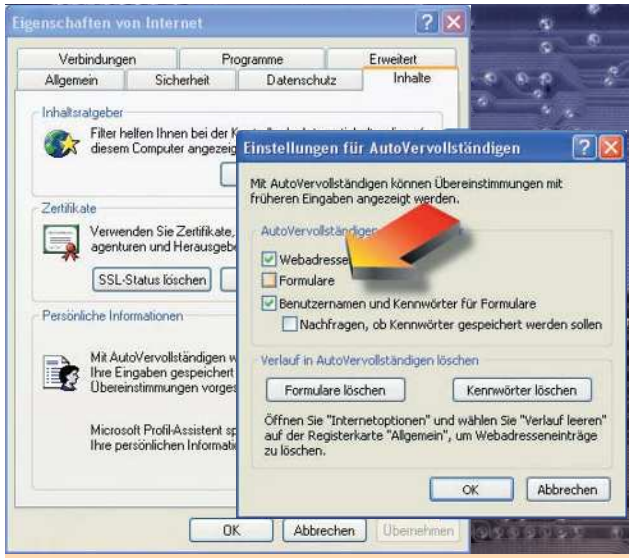
SCHWIERIGKEIT: FÜR EINSTEIGER

Ein zweites vom Internet Explorer „standardmäßig“ aufgebautes Sicherheitsrisiko ist das „AutoVervollständigen“. Dabei werden vom Benutzer gemachte Eingaben je nach Speicherung automatisch um den fehlenden Anteil ergänzt. Eigentlich eine sinnvolle Einrichtung, allerdings speichert der Explorer von sich aus auch Kennwörter und Benutzernamen (Nicknames oder Zugangsdaten). Die entsprechende Einstellung finden Sie ebenfalls in den „Internetoptionen“, hier jedoch unter der Registerkarte „Inhalte“. Dort befindet sich der Button „AutoVervollständigen“. Über ihn gelangen Sie in den Voreinstellungsbereich. Sie sollten hier unbedingt das Häkchen vor dem Eintrag „Benutzernamen und Kennwörter für Formulare“ durch Anklicken entfernen, wenn Sie verhindern möchten, dass der Explorer diese Daten für das automatische Vervollständigen einer Eingabe speichert.

Fazit: Unter allen Kandidaten besitzt der Internet Explorer die schlechtesten Sicherheitseigenschaften, aber auch die einfachste Konfiguration derselben. Trotzdem gilt: Wer den Explorer einsetzt, sollte zusätzlich über einen guten Virenscanner und eine gute Firewall verfügen. (*jb*)



2 KEIN ACTIVEX Aus Sicherheitsgründen sollten Sie ActiveX in den Sicherheitseinstellungen unbedingt deaktivieren.

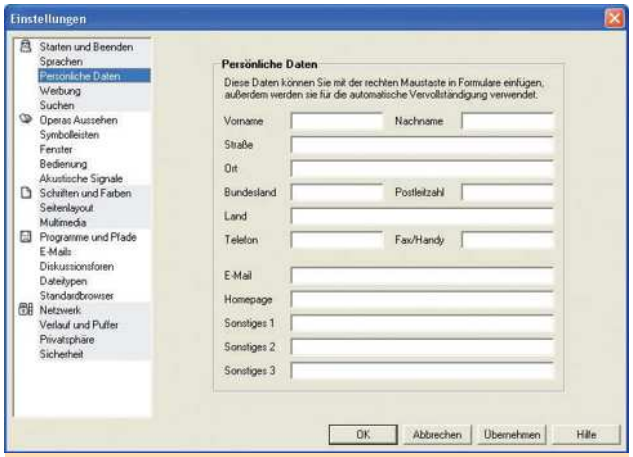


3 DATEINAMEN Um genau zu wissen, was sich hinter einem Attachment verbirgt, sollten Sie Dateinamen vollständig anzeigen lassen.

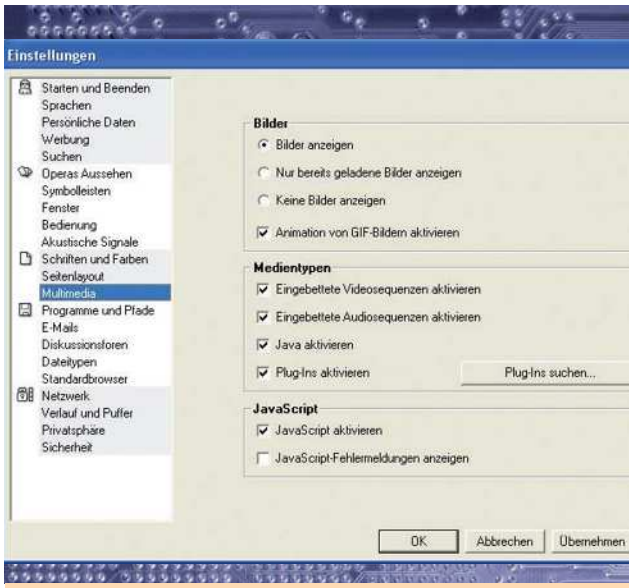
Opera, die Alternative!

Opera gehört zu den bekanntesten Browsern - und zu denen, die es gegenüber den „Platzhirschen“ Netscape und Internet Explorer nie leicht hatten. Was angesichts der Funktionen aber unverständlich ist.

Die aktuelle Opera-Version hat sich zu einem vollwertigen Mitglied der Browser-Familie gemausert. Vom Programmumfang her kann es der Browser aus dem Norden ohne Probleme mit den beiden „Großen“ aufnehmen. Auch das Thema Sicherheit spielt bei Opera eine entsprechende Rolle.



1 PRIVATSPHÄRE Um „User-Tracking“ zu vermeiden, geben Sie bei den persönlichen Daten lieber zu wenig als zu viel ein.



3 BROWSER-STEUERUNG Javascript sowie weitere Plug-Ins lassen sich in Opera über den Bereich Multimedia zu- oder abschalten.

Tipp 1: Persönliche Daten freilassen

SCHWIERIGKEIT: FÜR EINSTEIGER

Opera bietet viele Funktionen und Besonderheiten für den Websurfer, es gibt allerdings auch einige Eigenheiten, die man innerhalb der Einstellungen beachten sollte. Eine davon ist das User-Profil, das ein komplettes Datenpaket aus den persönlichen Adressdaten des Benutzers enthält, die per rechtem Mausklick automatisch auf Webformularen eingetragen werden. Diese Daten schließen allerdings auch Einträge wie Telefonnummer, Handy und so weiter mit ein. Opera „versteckt“ diese Daten zwar innerhalb seiner Programmstruktur, jedoch ist es möglich, die Daten an Stellen weiterzugeben, die sie zu Werbezwecken missbrauchen.

Tipp 2: Werbeprofil verhindern

SCHWIERIGKEIT: FÜR EINSTEIGER

Opera 6.04 – die aktuelle Version – ist ein kostenloses Browsersystem. Allerdings versucht der Hersteller den Benutzer für Werbezwecke einzuspannen, indem ihm unter der Rubrik „Werbung“ in den „Einstellungen“ ein Profil vorgegeben wird, in dem er seine Vorlieben für das Internet auswählt. Dieses „User-Tracking“ ermöglicht es kommerziellen Webangeboten, einen genau auf den entsprechenden Benutzer zugeschnittenen Inhalt anzuzeigen. Lassen Sie die entsprechenden Eingabefelder der Kategorie „Werbung“ in den „Einstellungen“ frei, wenn Sie nicht möchten, dass diese und andere persönliche Daten an Dritte weitergegeben werden sollen.

Tipp 3: Java/Javascript deaktivieren

SCHWIERIGKEIT: FÜR EINSTEIGER

Opera kann wahlweise mit oder ohne Java-Unterstützung installiert werden. Je nach Inhalt können Java-Applets auch schädliche Auswirkungen haben. Soll dem von Grund auf vorgebeugt werden, sollten Sie Java und Javascript innerhalb von Opera abschalten. Zu finden sind die entsprechenden Einstellungen unter dem Eintrag „Multimedia“. Durch Setzen oder Löschen der Checkmarken aktivieren oder deaktivieren Sie die entsprechenden Einträge.

Tipp 4: Cookies deaktivieren oder selektieren

SCHWIERIGKEIT: FÜR EINSTEIGER

Die Cookie-Behandlung von Opera befindet sich in den Einstellungen unter der Kategorie „Privatsphäre“. Cookies sind von Opera standardmäßig aktiviert, das heißt, dass jede Webseite automatisch Cookies im Ordner für temporäre Internetdaten speichern kann. Durch Löschen der Checkmarke wird diese Funktion abgeschaltet. Damit sind allerdings notwendige Cookies wie zum Beispiel die der Webshops ebenfalls gesperrt. Der Button „Bearbeiten der Serverfilter …“ führt in einen Unterbereich, in dem Sie festlegen können, welche Webseiten Cookies setzen dürfen.

Fazit: Opera ist ein guter Browser. Die Fallstricke bei den persönlichen Angaben kann man umschiffen, indem man die jeweiligen Felder frei lässt. (*jb*)

Auf Überholspur: Mozilla

Das Open-Source-Projekt „Mozilla" hat sich zu einem vollwertigen Browsersystem entwickelt, dass sich hinter seinen Konkurrenten nicht mehr zu verstecken braucht – auch beim Thema Sicherheit.

Der größte Vorteil von „Mozilla" ist seine Kompaktheit und ressourcensparende Programmierung, im Test lief das komplette Browsersystem inklusive eines Flash-Plug-Ins von einer 32-Megabyte-CompactFlash-Card im Card-Reader des Test-PCs. Dafür bietet Mozilla auch nicht so umfangreiche Programmerweiterungen, was aber nicht unbedingt negativ zu bewerten ist.

Tipp 1: Wichtige Einstellungen

SCHWIERIGKEIT: FÜR EINSTEIGER

Die Einstellungen für den Browser finden sich im Menü „Bearbeiten" und dem Menüpunkt „Einstellungen …". Sie unterteilen sich in verschiedene Kategorien, wichtig sind hier vor allem die Bereiche „Datenschutz und Sicherheit", sowie „Erweitert". Sie enthalten die Grundeinstellungen für Sicherheitsregeln, nach denen der Browser im Internet mit Webinhalten verfahren soll. Im oberen Bereich „Datenschutz …" finden Sie Einstellungen für die Cookie-Behandlung, Passwörter und Formulare. Sie können in dem Unterbereich „Master-Passwort" ein spezielles Kennwort angeben, das alle weiteren Passwörter nur nach Eingabe der entsprechend festgelegten Kennung freigibt.

Tipp 2: „Passwort speichern" abschalten

SCHWIERIGKEIT: FÜR EINSTEIGER

Sollen Passwörter vom Browser nicht gespeichert werden, so wechseln Sie innerhalb der Mozilla-Einstellungen auf den Bereich „Datenschutz" und dann auf „Passwörter". Entfernen Sie die Checkmarke bei der Option „Passwörter speichern".

Tipp 3: Javascript-Aktivierung einstellen

SCHWIERIGKEIT: FÜR EINSTEIGER

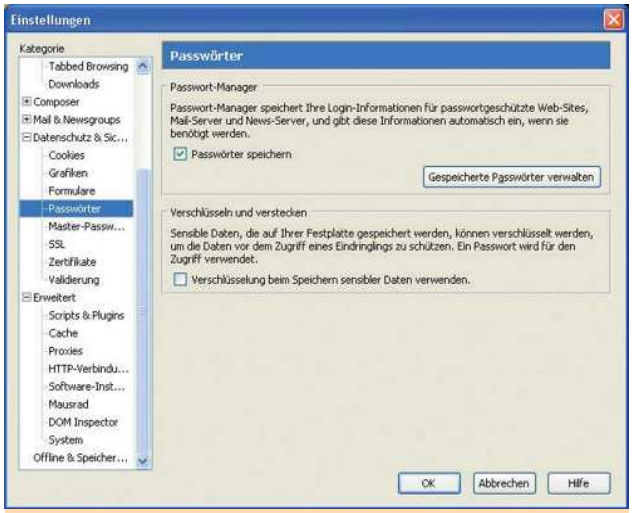
Im Einstellungsbereich „Erweitert", Unterbereich „Scripts und Plug-Ins" finden Sie eine Eintragsliste für die Aktivierung von JavaScript unter bestimmten Voraussetzungen. Diese Voraussetzungen sind standardmäßig alle „gesetzt", so dass Javascripts auf Webseiten ungehinderten Zugriff erhalten. Dazu gehört zum Beispiel der obere Eintrag „Nicht angeforderte Fenster öffnen". Auf diese Weise werden die so genannten Pop-Up-Fenster gerne geöffnet, die zum Beispiel bei Mouse-Handler wie „OnClick" oder „OnMouseOver" sofort weitere Pop-Ups aufmachen. Durch Entfernen der Checkmarke wird das automatische Öffnen durch Scripts unterbunden. Auch das Setzen und Erzeugen von Cookies durch Javascripts lässt sich hier unterbinden.

Tipp 4: History löschen

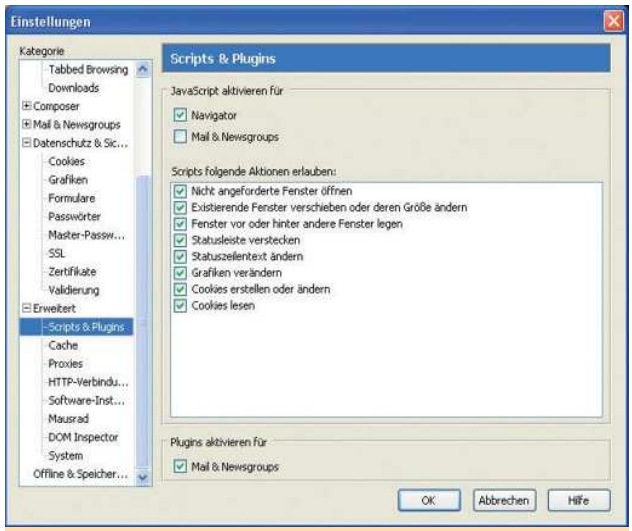
SCHWIERIGKEIT: FÜR EINSTEIGER

Da jeder Web-Besuch Spuren hinterlässt, die von Webseiten-Betreibern auf vielfältige Art ausgewertet werden können, ist es sinnvoll, die Anzahl der Spuren so niedrig wie möglich zu halten. Dazu gehört auch das Löschen der History-Einträge. Innerhalb von Mozilla ist die History unter der Rubrik „Navigator" zu finden. Mozilla speichert einmal Einträge der Browser-History und Einträge der Adressleiste. Diese werden für eine von Ihnen frei definierbare Anzahl von Tagen gespeichert und über die Buttons auf der rechten Seite des Fensters gelöscht.

Fazit: Die Sicherheitseinstellungen unter Mozilla sind ausreichend. Vor allem die Script- und Plug-In-Verwaltung sind wesentlich besser als beim Explorer. Auch ist die Gefahr durch ActiveX-Kontrollen „gelenkt" zu werden, ist löblicherweise nicht gegeben. (*jb*)



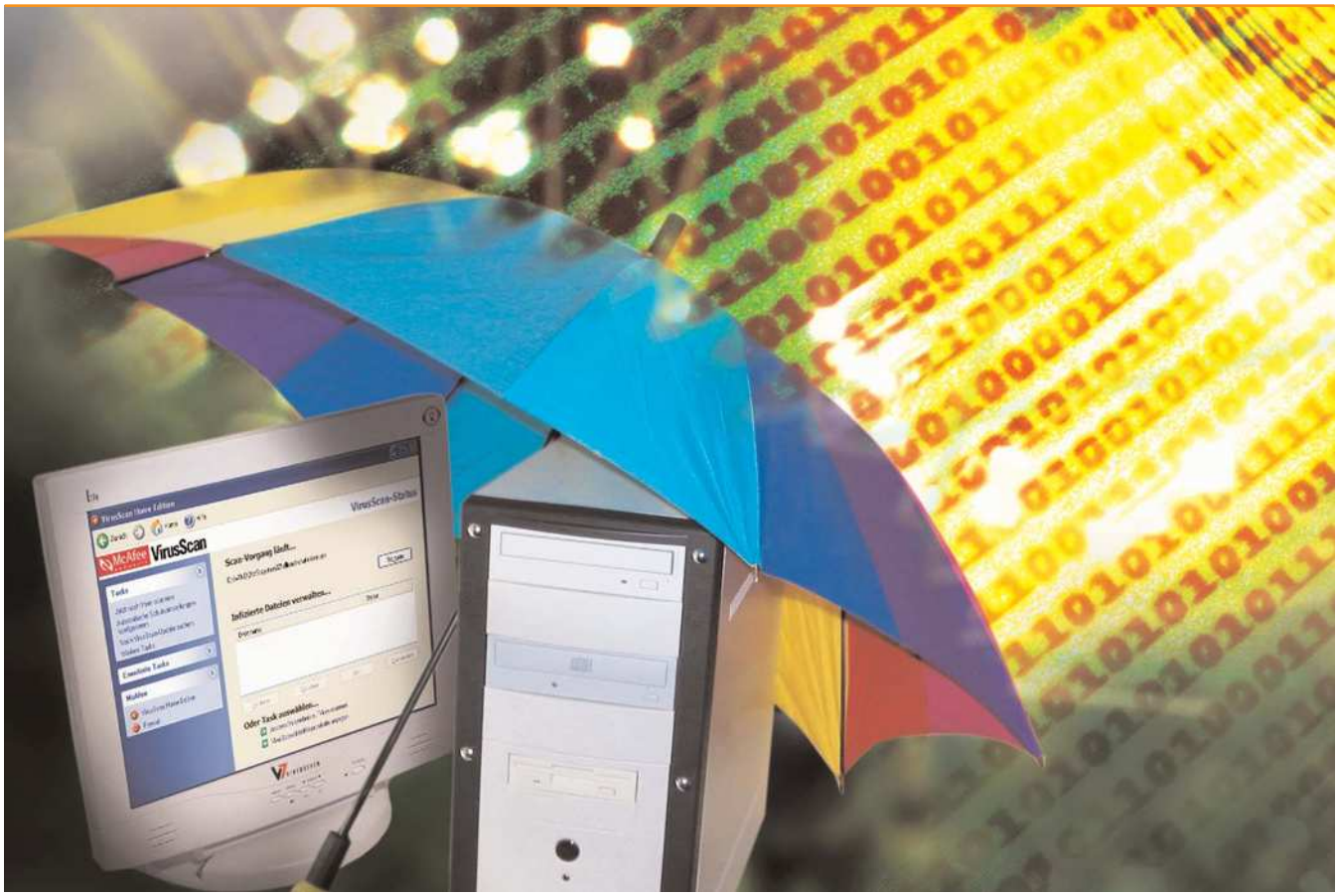
2 PASSWORT-MANAGER Durch Festlegen der Passwort-Einträge verhindern Sie, dass Kennwörter innerhalb von Mozilla gespeichert werden.



3 JAVASCRIPT Die Javascript-Verwaltung legt fest, wann Scripte auf Webseiten auf den Browser zugreifen dürfen und wann nicht.

8 Virenscanner und Firewalls im Test

Digitaler Schutz



Nicht nur Frodo aus dem Auenland braucht verlässliche Gefährten, auch jeder Windows-Anwender sollte sich zum Schutz vor Viren den passenden „Gefährten" installieren.

Seit das Internet in unser Leben gekommen ist, haben sich auch die Viren verändert. Klassisches Ungeziefer, das andere Programme mit dem eigenen Code infiziert, treffen Sie nur noch selten an. Auch die früher so gefürchteten Makroviren haben ihre Zähne verloren. Die eigentliche Gefahr kommt – wie soll es auch anders sein – aus dem Internet: So genannte Würmer bedrohen heutzutage Windows-Installationen. Diese Fieslinge nisten sich über Sicherheitslücken im Windows als eigenständige Programme im System-Ordner ein. Wer sich hier auf Microsoft verlässt und nur alle Patches und Bugfixes installiert, der ist verlassen. Wirklich effektiven Schutz bieten nur Virenscanner. Daher haben wir uns vier bekannte Ungeziefervernichter ins Labor geholt: Norton Antivirus 2003, Mcafee Virusscan 7.0, Panda Antivirus Titanium und das für Privatanwender kostenlose Programm Antivir Personal Edition. Die Leistungsfähigkeit hat für uns die Firma GEGA IT-Solutions ermittelt.

Der Erkennungstest für die weit verbreiteten Viren (ITW = in the wild, deutsch: in freier Wildbahn) wurde anhand der Wildlist 11/2002 durchgeführt. Diese Liste (www.wildlist.org) basiert auf den Angaben von 70 Virenforschern weltweit und enthält Informationen darüber, welche Viren zurzeit bei Anwendern auftreten. Die vier Virenscanner wurden unter Windows XP mit 520 verschiedenen infizierten Dateien getestet. Alle Programme können sowohl On-Demand (Scanner-Suchlauf) als auch On-Access (Virenwächter) alle in

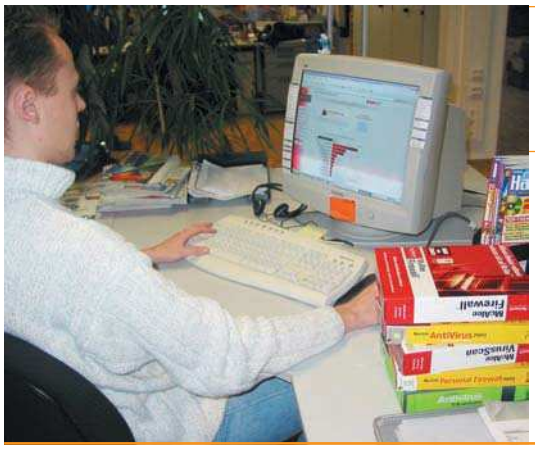
WAS IST?

Viren
Viren sind kleine „Sabotage"-Programme, die sich an andere ausführbare Dateien hängen.

Würmer
Würmer verbreiten sich via Netzwerk selbsttätig von Computer zu Computer.

Makroviren
Makroviren verstecken sich in Word- oder Excel-Dateien. Sie bestehen aus Programmbefehlen.

Ports
Werden verwendet, um die Kontaktaufnahme von PCs in einem Netzwerk zu ermöglichen.



Test-Philosophie: Virenschutz

Virenscanner und Firewall-Software erfordern komplexe Tests und ein entsprechendes Wertungsverfahren.

TESTVERFAHREN

Mithilfe der Messergebnisse der Firma GEGA IT-Solutions bewerten wir die Programme.

Bei der **Ausstattung (20 %)** achten wir auf die Sprachversion von Programm und Handbuch sowie Virendefinition-Updates. Bei den **Eigenschaften (20 %)** geht es vorrangig um die Bootfähigkeit der CD und um die Möglichkeit zur Erstellung von Notfallsdisketten. Die **Leistung (60 %)** der Programme ermitteln wir mithilfe der Firma GEGA IT-Solutions. Das Magdeburger Unternehmen testet Virenscanner anhand der 520 am meisten verbreiteten Viren und untersucht auch, welche Archive von der Software durchsucht werden können. Die Firewall-Programme installieren wir auf einem PC mit DSL-Anschluss und prüfen diese mithilfe von spezieller Software und Webdiensten.

den Dateien verborgenen Viren aufspüren. Nur Antivir PE identifizierte während des Suchlaufes keine Bootviren auf infizierten Disketten. H+BEDV Datentechnik hat bereits ein Update angekündigt, um den Fehler zu beheben.

Die Erkennung der verschiedenen Archivformate funktionierte jedoch nicht ganz reibungslos: Während alle Virenscanner noch ARJ, CAB, LHA und ZIP durchsuchen, schwächelt Norton Antivirus 2003 schon bei RAR – Ungeziefer in solchen Archiven findet das Programm nicht. Mit den in der Spieleszene beliebten ACE-Archiven kommen nur Mcafee Virusscan 7.0 und Panda Antivirus Titanium klar. Sollten Sie Linux beispielsweise als Internet-Gateway/-Router verwenden, dann interessieren Sie die Ergebnisse der Unix-Archivformate: Nur Mcafee und Panda durchsuchen alle Formate, darunter Bzip2 (BZ), Tar und Gnuzip (GZ) (auch verschachtelt). Werden dem Scanner passwortgeschützte Archive vorgesetzt, bemängelt nur Antivir, dass es ein Archiv nicht nach Viren untersuchen konnte. Alle anderen Programme übergehen ein solches nicht durchsuchbares Archiv kommentarlos.

Per E-Mail oder IRC wird heute sehr häufig versucht, dem Anwender Trojaner oder Backdoors unterzujubeln. Da die Virenscanner die Standard-Backdoors wie Netbus, Sub7 oder Backorifice problemlos erkennen, werden sie häufig in laufzeitkomprimierter Form gespeichert – ähnlich wie ein ZIP-Archiv komprimiert, aber die Datei ist weiterhin direkt per Doppelklick startbar. Virenscanner können die Datei nun oft nicht mehr erkennen und der Test, ob sie verschiedene Packformate beherrschen, zeigt, dass alle getesteten Programme noch deutliche Lücken aufweisen. Der absolute Negativ-Spitzenreiter ist Norton Antivirus 2003: Nicht ein einziges Win32-Kompressionsformat (laufzeitkomprimierter Trojaner) wird erkannt. Ähnlich traurig sieht es bei Panda und bei Antivir aus. Nur Mcafee unterstützt immerhin die Hälfte der getesteten Win32-Formate. DOS-Formate (16 Bit) wurden der Vollständigkeit halber mitgetestet, sollten heutzutage aber kaum noch eine Rolle spielen (siehe auch Tabelle). Einzelheiten über Mcafee Virusscan 7.0 erfahren Sie im Einzeltest, alle anderen Virenscanner folgen hier:

Antivir Personal Edition: Antivir ist kostenlos erhältlich (siehe Heft-CD) und schon deshalb einen Tipp wert. Nur das kleine Problem mit den Bootviren trübt die Freude ein wenig, doch dieses Problem soll laut Hersteller schnell behoben werden. Was wirklich stört, sind aber die Updates: Neue Virensignaturen machen sich mit einem 1,5 Megabyte großen Download bemerkbar und erscheinen meist wöchentlich; neue Programmversionen sind dagegen oft drei bis vier Megabyte groß und werden bis zu einmal im Monat veröffentlicht. Daher ist Antivir eher etwas für Anwender mit einem Breitband-Internetanschluss oder einer Flatrate.

Norton Antivirus 2003: Knapp 50 Euro möchte Symantec für den Virenscanner haben, der damit der teuerste Testkandidat ist. Im Vergleich mit den anderen Programmen kann Norton Antivirus 2003 lediglich in der Benutzeroberfläche punkten. In allen anderen Bereichen war er deutlich schlechter als die Konkurrenz. Zwar findet er alle weit verbreiteten Viren, aber schon einige bekannte Archivformate wie ACE oder RAR bringen den Scanner aus dem Trab. Laufzeitkomprimierte Dateien sucht Norton erst gar nicht. Updates machen sich mit deutlich unter 100 KB pro Woche bemerkbar.

Panda Antivirus Titanium: Bereits für 33 Euro bekommen Sie die Titanium-Version von Panda Antivirus. Damit hat das Programm fast den gleichen Preis wie Mcafee, trotzdem ist der Platzhirsch in einigen Punkten etwas besser. Es geht genügsamer mit den Systemressourcen um, belegt aber trotzdem noch 40 MB an Speicherplatz. Für Modembesitzer interessant: Die täglichen Updates sind mit nur zwei bis fünf KB sehr klein. Aber Vorsicht: Panda Antivirus Titanium löscht Viren automatisch, der Benutzer hat keinen Einfluss auf die Vorgehensweise des Scanners. So könnten auch nichtinfizierte Dateien beschädigt werden.

Firewalls: Ein Virenscanner alleine bietet noch nicht die optimale Sicherheit, Sie sollten zusätzlich eine Firewall-Software installieren. Solch ein Programm filtert den gesamten Netzwerk- und Internetverkehr, so dass

Typ-beratung

Alles Wissenswerte zum Thema Virenscanner

Kann mein Virenscanner bisher unbekannte Viren aufspüren?
Theoretisch kann ein Virenscanner mithilfe der Heuristik auch Viren aufspüren, die nicht in der Datenbank gelistet sind. Dazu wird nach verdächtigen Operationen gescannt, beispielsweise nach dem Versuch, die Festplatte zu formatieren oder eine Systemdatei zu löschen. In der Praxis funktioniert dieses Verfahren nur mangelhaft, daher sollten Sie Ihren Virenscanner immer auf dem neuesten Stand halten und regelmäßig aktuelle Virendefinitionsdateien herunterladen.

Was ist, wenn mein System nicht mehr startet?
Viele Virenscanner besitzen eine Funktion zur Erstellung von Notfalldisketten. Mit diesen können Sie ein „zerstörtes" System nach Viren durchsuchen. Die CDs von Norton Antivirus 2003 und Mcafee Virusscan 7.0 sind sogar bootfähig. Allerdings können die zwei Virenscanner nur FAT-Dateisysteme lesen, NTFS wird nicht unterstützt. Die beiden Programme scannen nach dem Booten vom CD-Laufwerk die Festplatte nach bekanntem Ungeziefer und entfernen es gegebenenfalls. Mcafee bietet die Dateien für die Notfalldiskette auch online an, damit Sie mit den aktuellen Virendefinitionen arbeiten können.

Programme nur mit Ihrer Erlaubnis Daten ins Internet senden dürfen. Firewalls sollen auch Angreifer von außen abwehren. Besonders wichtig ist, dass die Software NetBIOS-Ports (137 bis 139) für den Zugriff aus dem Internet blockiert. Dadurch sind eventuell freigegebene Ressourcen auch von außen unsichtbar. Zum Test haben wir die Programme Norton Personal Firewall 2003, Mcafee Firewall 4.0, Zonealarm 3.1.395 und Personal Firewall 5.0 Build 1150 antreten lassen. Die letzten beiden Programme sind für Privatanwender kostenlos.

Alle vier Programme blockieren die NetBIOS-Ports so, dass die Windows-Freigaben nicht mehr sichtbar sind. Versucht ein Angreifer, Ihren Rechner nach offenen Ports zu scannen, schlagen alle Firewalls bis auf die von Sygate sofort an. Mcafee und Symantec bieten sogar die Möglichkeit, den Angreifer zurückzuverfolgen. Sollten Sie sich einen Trojaner eingefangen haben, so wird zwar der Verkehr zwischen Server und Trojaner von allen Programmen blockiert, aber nur Zonealarm, Norton Personal Firewall 2003 und Mcafee Firewall 4.0 melden, dass es sich um einen Eindringling handelt. Mithilfe eines Testprogramms haben wir versucht, offene Ports bei jeder Firewall-Software zu finden. Alle sind wasserdicht, nur bei der Sygate Personal Firewall tritt in der Standard-Konfiguration Folgendes auf: Die Ports 135 und 5.000 sind von außen offen. Letzterer ist für UPnP (Universal Plug and Play) zuständig. Er wird für Internet Connection Sharing benötigt. Trotzdem sollten diese Ports zur Sicherheit geschlossen sein. Weitere Details über Norton Personal Firewall 2003 finden Sie im Einzeltest.

Zonealarm 3.1.395: Diese Firewall steht leider nur in Englisch zur Verfügung, auch die Dokumentation, die im Netz abgerufen werden kann, ist in englischer Sprache. Dafür ist Zonealarm kostenlos und lässt sich sehr einfach bedienen. Auch mit Online-Spielen hat die Firewall keine Probleme. Versucht ein Angreifer Ihren Rechner nach offenen Ports zu scannen, erstellt Zonealarm für jeden Port eine Meldung. Dies kann auf die Dauer nerven, daher sollten Sie dies nur protokollieren lassen und die Meldung abschalten.

Personal Firewall 5.0: Auch das Sygate-Produkt steht nur in Englisch bereit, ist aber auch für Privatanwender kostenlos. Leider zeigt das Programm kleine Schwächen gegenüber den anderen Firewalls im Testfeld. Die Konfiguration der Personal Firewall 5.0 kann wie bei Norton mit einem Passwort geschützt werden. Dies kann sehr nützlich sein, damit kein Unbefugter an Ihrem Rechner Ports für Trojaner öffnen kann.

Mcafee Firewall 4.0: Das Programm wird komplett in deutscher Sprache angeboten. Während der Installation wird die Festplatte nach Programmen mit Internetambitionen durchsucht und diese werden angezeigt. Die Firewall bietet auch eine Risikoeinschätzung, damit Sie selbst bewerten können, ob das angezeigte Programm eine Verbindung zum Internet aufbauen darf. MARCO ALBERT

ANSICHTSSACHE

Viren, Würmer und Trojaner sind reale Gefahren, denen jeder PC-Nutzer mit Internetanschluss täglich ausgesetzt ist. Daher sollte entsprechende Software zum Schutz persönlicher Daten zur Standardausrüstung gehören. Dieser Test hat gezeigt, dass optimaler Schutz noch nicht mal teuer sein muss. Den Virenscanner Antivir und die Firewall Zonealarm gibt es sogar kostenlos! Übrigens sollten Sie für optimale Sicherheit sowohl Virenscanner als auch Firewall installieren. Wenn Ihr Programm keine Update-Funktion hat, empfiehlt sich zudem, Updates der Virendefinition im Auge zu behalten.

„Nur Virenscanner und Firewall zusammen bieten Schutz."

Frank Neupert
Redakteur
Bereich Sonderhefte

Überzeugend

Virenscanner: Mcafee Virusscan 7.0

aMcafee hat mit Virusscan 7.0 den besten Virenscanner im Testfeld programmiert; er zeigt keine Schwächen bei der ITW-Erkennung.

MCAFEE VIRUSSCAN 7.0 Der Scanvorgang dauert 330 Sekunden.

Vor allem Anwender, die einen einfach zu bedienenden Virenscanner suchen, werden mit Mcafee Virusscan 7.0 glücklich sein. Sie müssen sich praktisch um nichts kümmern. Updates werden automatisch gemacht und sind mit 35 bis 70 KB auch für Modem-Besitzer kein Problem. Von den laufzeitkomprimierten Dateien erkennt Mcafee immerhin die Hälfte, laut Firmenaussage soll dies mit einem neuen Update in den nächsten Tagen noch besser werden. Auch die Zusammenarbeit mit gängigen E-Mail-Programmen klappt reibungslos. Sollten doch einmal Probleme auftreten, steht Ihnen per Chat, E-Mail oder Telefon ein kompetentes Expertenteam zur Verfügung. Die 35 Euro sind für den Mcafee Virusscan 7.0 gut angelegt. *(ma)*

Mcafee Virusscan 7.0		
Hersteller: Netw. Associat.	Ausstattung:	1,3
Preis: € 35,-	Eigenschaften:	1,5
Webseite: de.mcafee.com	Leistung:	2,3
Preis-Leistung: Befried.	GESAMT	2,0

Teurer Schutz

Firewall: Norton Personal Firewall 2003

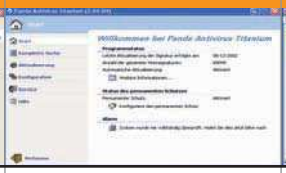
Norton Personal Firewall 2003 bietet zwar optimalen Schutz vor Angreifern aus dem Netz und umfangreiche Optionen, aber der Preis ist ein wenig hoch.

PERSONAL FIREWALL 2003 Mit „Visual Tracking" verfolgen Sie Angreifer.

Nach der Installation begrüßt Norton den Anwender mit einem Assistenten, der auf Wunsch eine Vorkonfiguration übernimmt. So kann dieser den Rechner nach Anwendungen untersuchen, die eine Internet-Verbindung erfordern. Spätere Konfigurationsversuche werden durch die etwas unübersichtliche Bedienoberfläche behindert. Zwar besticht Norton Personal Firewall 2003 durch viele Funktionen, doch Sie müssen ein wenig Zeit dafür aufbringen, um sich durch die Menüstrukturen des Programms zu kämpfen. Immerhin bietet Symantec dafür ein Lernprogramm. Knapp 50 Euro für eine Firewall-Software ist kein Schnäppchen. Trotzdem bekommen Sie ein sehr gutes Programm. *(ma)*

Norton Personal Firewall 2003		
Hersteller: Symantec	Ausstattung:	1,3
Preis: € 49,95	Eigenschaften:	2,2
Webseite: www.symantec.de	Leistung:	1,2
Preis-Leistung: Befried.	GESAMT	1,4

VIREN-SCANNER

	Mcafee Virusscan 7.0	Panda Antivirus Titanium	Antivir Personal Edition	Norton Antivirus 2003
				
☐ Hersteller	Network Associates	Panda Software	H+BEDV Datentechnik	Symantec
☐ Info-Telefon	(089) 3 70 70	(02065) 98 76 54	(07542) 9 30 40	(02102) 7 45 30
☐ Webseite	de.mcafee.com	www.panda-software.de	www.free-av.de	www.symantec.de
☐ Preis	€ 35,-	€ 33,-	Kostenlos	€ 49,95
☐ Preis/Leistung	Befriedigend	Befriedigend	Sehr gut	Mangelhaft
AUSSTATTUNG	**1,3**	**1,7**	**2,3**	**1,3**
☐ Update-Berechtigung	Ja	Ja	Ja	Ja
☐ Sprache Programm	Deutsch	Deutsch	Deutsch	Deutsch
☐ Dokumentation	Handbuch	Handbuch (Heft)	Online	Handbuch
☐ Bezugsquelle	Handel	Handel	Online	Handel
EIGENSCHAFTEN	**1,5**	**2,3**	**3,0**	**1,3**
☐ Bedienung	Einfach	Einfach	Einfach	Einfach
☐ Bootfähige CD	Nein	Nein	Nein	Ja
☐ Notfalldisketten erstellbar	Ja	Ja	Nein	Ja
☐ Wächterfunktionalität	Ja	Ja	Ja	Ja
LEISTUNG	**2,3**	**2,7**	**2,3**	**3,5**
☐ Virenerkennung ITW (On Demand)	100 Prozent	100 Prozent	95,8 Prozent	100 Prozent
☐ Virenerkennung ITW (On Access)	100 Prozent	100 Prozent	100 Prozent	100 Prozent
☐ Unterstützte Archive	ACE, ARJ, CAB, LHA, RAR, ZIP	ACE, ARJ, CAB, LHA, RAR, ZIP	ARJ, CAB, LHA, RAR, ZIP	ARJ, CAB, LHA, ZIP
☐ Passwortgeschütze Archive?	Werden übergangen	Werden übergangen	Werden gemeldet	Werden übergangen
☐ Windows (32 Bit) Laufzeitkomprimierung	Erkennt 4 von 8	Erkennt 1 von 8	Erkennt 2 von 8	Erkennt 0 von 8
☐ DOS (16 Bit) Laufzeitkomprimierung	Erkennt 3 von 5	Erkennt 3 von 5	Erkennt 1 von 5	Erkennt 1 von 5
FAZIT	**GESAMT**	**GESAMT**	**GESAMT**	**GESAMT**
	Mcafee überzeugt durch gute Trojaner- und Viren-Erkennung **2,0**	Für Einsteiger eine gute Alternative, da einfach bedienbar **2,4**	Virenscanner mit sehr gutem Preis-Leistungs-Verhältnis **2,5**	Teuer und viele Probleme mit komprimierten Dateien **2,6**

FIREWALL

	Norton Pers. Firewall	Mcafee Firewall 4.0	Zonealarm 3.1.395	Personal Firewall 5.0
☐ Hersteller	Symantec	Network Associates	Zonelabs	Sygate Technologies
☐ Info-Telefon	(02102) 7 45 30	(089) 3 70 70	(06196) 77 36 70	+1 (510) 7 42 26 00
☐ Webseite	www.symantec.de	de.mcafee.com	www.zonelabs.com	www.sygate.com
☐ Preis	€ 49,95	€ 39,57	Kostenlos	Kostenlos
☐ Preis/Leistung	Befriedigend	Befriedigend	Sehr gut	Gut
AUSSTATTUNG	**1,3**	**1,3**	**2,7**	**2,7**
☐ Betriebssysteme	Windows 9x, Me, 2000, XP	Windows 9x, Me, 2000, XP	Windows 9x, Me, NT, 2000, XP	Windows 9x, Me, NT, 2000, XP
☐ Sprache Programm	Deutsch	Deutsch	Englisch	Englisch
☐ Dokumentation	Deutsches Handbuch	Deutsches Handbuch	Online, Englisch	Online, Englisch
EIGENSCHAFTEN	**2,2**	**3,0**	**3,0**	**2,2**
☐ 0190-Dialer-Schutz	Nein	Nein	Nein	Nein
☐ Lernfähigkeit	Ja	Ja	Ja	Ja
☐ Passwortschutz	Ja	Ja	Nein	Ja
☐ Bedienung	Einfach	Sehr einfach	Sehr einfach	Einfach
☐ Log-Dateien	Ja (im Programm)	Ja (im Programm)	Ja (als Text-Datei)	Ja (im Programm)
LEISTUNG	**1,2**	**1,2**	**1,3**	**1,7**
☐ Filterfunktion ausgehend	Gut	Gut	Gut	Gut
☐ NetBIOS (Windows-Freigaben)	Nach außen nicht sichtbar	Nach außen nicht sichtbar	Nach außen nicht sichtbar	Nach außen nicht sichtbar
☐ Trojaner-Warnung	Ja	Ja	Ja	Nein
☐ Anzeige von Portscan	Ja (Angreifer kann zurückverfolgt werden)	Ja (Angreifer kann zurückverfolgt werden)	Ja	Ja
☐ Offene TCP-Ports	Keine	Keine	Keine	Ja (135 und 5.000)
☐ Probleme mit Online-Spielen	Nein	Nein	Nein	Nein
FAZIT	**GESAMT**	**GESAMT**	**GESAMT**	**GESAMT**
	Bietet optimalen Schutz und den besten Komfort im Testfeld **1,4**	Der Firewall von Mcafee fehlt ein Passwortschutz. **1,6**	Einfach bedienbar und auch noch kostenlos erhältlich **1,9**	Zwar kostenlos, aber nicht einfach zu konfigurieren **2,0**

Praxistest: Software

Virenscanner oder Firewall-Software kaufen und installieren – damit ist es oft nicht getan. Wir haben noch einige Tipps für den Umgang mit der Sicherheitssoftware für Sie.

Da Firewalls den gesamten Internetverkehr filtern, werden auch Multiplayer-Spiele blockiert. Norton Personal Firewall 2003 und Mcafee Firewall 4.0 durchsuchen nach der Installation die Festplatte nach Spielen. Diese werden dann nicht mehr blokkiert. Installieren Sie ein Spiel nachträglich oder nutzen Sie Zonealarm, dann müssen Sie das Online-Spiel nachträglich freigeben. Dazu starten Sie das Spiel und lassen es eine Verbindung zum Internet aufbauen. Anschließend wechseln Sie per „Alt“ und Tabulator zur Firewall und lassen die Verbindung zu. Setzen Sie gleich die Lernoption, damit sich das Programm die Auswahl fürs nächste Mal merkt.

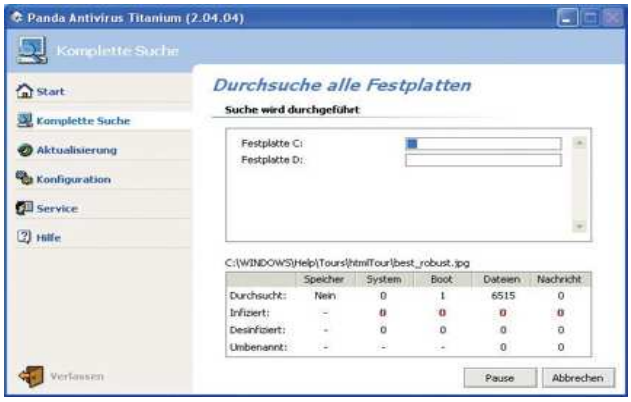
Damit erst gar kein Virus auf Ihr System kommt, müssen Sie die Wächterfunktion des Virenscanners aktivieren. Diese checkt jede Dateioperation (Kopieren, Löschen, Erstellen und Verschieben) auf Viren. Dazu klikken Sie das Symbol Ihres Virenscanners in der Systemleiste (neben der Uhr) doppelt an. Verwenden Sie Mcafee, so wird Ihnen direkt angezeigt, ob der Wächter aktiv ist. Auch bei Panda Antivirus finden Sie die Option für die Dateiüberwachung auf der ersten Seite. Sollten Sie Norton Antivirus einsetzen, dann müssen Sie zunächst auf „Option“ klicken. Anschließend können Sie unter „Auto-Protect aktivieren (empfohlen)“ den Wächter ein- beziehungsweise ausschalten. Beim Einsatz von Antivir müssen Sie das Hauptprogramm über die Startleiste starten und unter „Option“ auf „Konfigurationsmenü“ klicken. Nun rufen Sie „Diverses“ auf, hier können Sie mit „Guard beim Systemstart laden“ den Wächter aktivieren.

Für den Fall, dass das System gar nicht mehr startet, ermöglichen die Virenscanner das Erstellen von Notfalldisketten. Mcafee bietet für diesen Zweck ein spezielles Dienstprogramm an, das automatisch eine Bootdiskette erstellt. Zudem ist auch die Installations-CD von Mcafee bootfähig. Auch von der Norton-Antivirus-CD wird ein Betriebssystem gestartet und es werden alle Laufwerke nach Viren durchsucht.

Alle getesteten Virenscanner lassen sich automatisch oder innerhalb des Programms mit einer neuen Virendefinition versorgen. Dazu ist allerdings eine Internetverbindung notwendig. Es soll aber noch Rechner geben, die keinen Zugang zum weltweiten Netz haben. Für solche PCs können Sie die Virendefinition auch manuell von der Hersteller-Webseite herunterladen. Symantec bietet gleich auf der Startseite der Homepage einen Downloadlink zur aktuellen Virendefinitionsdatei an. Panda erlaubt nur registrierten Anwendern das Herunterladen von neuen Virensignaturen. Dazu klicken Sie auf der Webseite auf „Support“ – „Update“ – „Intelligent Updates“. Bei Antivir muss die Version der Definitionsdatei immer mit der Version des Hauptprogramms übereinstimmen. Die Files bekommen Sie unter „Download“. Nur Mcafee bietet für Virusscan 7.0 kein manuelles Update der Virensignaturen an. Sie müssen dieses immer über das Programm selbst auslösen.

MARCO ALBERT

NORTON ANTIVIRUS 2003 Damit sich erst gar keine Viren auf dem System einschleichen, müssen Sie den Wächter durch „Auto-Protect“ aktivieren.

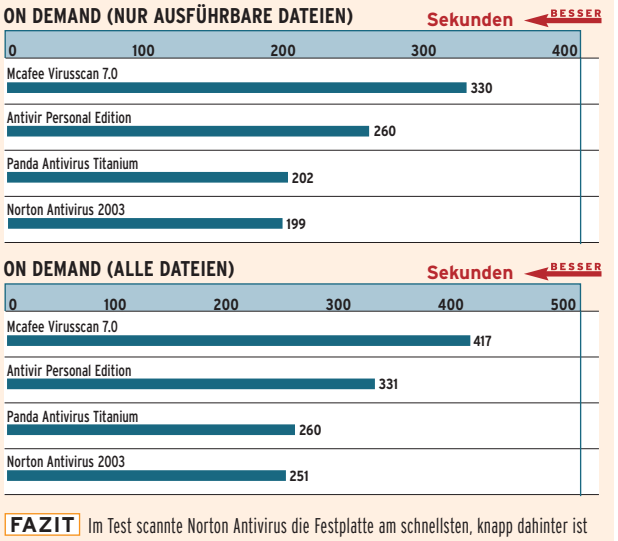


PANDA ANTIVIRUS TITANIUM Nach der Installation des Virenscanners sollten Sie alle Laufwerke auf Ungeziefer prüfen lassen.

Vergleich Virenscanner

Settings: Intel Pentium III 1.000 MHz, Intel BX-Chipsatz, 256 MB SDR-SDRAM, 15-GB-Festplatte mit 5.400 U/min, circa 20.000 Dateien

LEGENDE Scanzeit



FAZIT Im Test scannte Norton Antivirus die Festplatte am schnellsten, knapp dahinter ist Panda Antivirus Titanium. Mcafee Virusscan 7.0 benötigte die meiste Zeit.

Eine sichere Entscheidung:

ATELCO 4home!

AMD Athlon 2000+ 256 MB, 60 GB HDD, 64 MB VGA

5 JAHRE ATELCO-GARANTIE auf Ihren PC!

RABATT BEI VERSAND-ZUSTELLUNG! **3%**

28 TAGE Rückgaberecht

Wir bieten Ihnen auf alle Artikel 28 Tage Rückgaberecht. Die Ware muss originalverpackt, vollständig und ungebraucht sein. Dienst- und Serviceleistungen sind von der Rücknahme ausgeschlossen. Bei zwischenzeitlichen Preissenkungen erfolgt die Gutschrift zum Tagespreis.

■ Mini-Tower ATX, 300W Netzteil ■ **MSI KT4V-L, Socket A Mainboard** ■ **AMD Athlon XP 2000+** (QuantiSpeed Technologie: Taktfrequenz 1,667 GHz) ■ Arctic Cooling 2500pro SuperSilent ■ 3.5" Floppy-Laufwerk 1.44 MB ■ 256MB DDR DIMM PC2700/333 MHz ■ Samsung SV6003H, 60 GB ■ 6-Kanal Sound on Board ■ **MSI G4MX440SES/T 64MB SDRAM, nVidia Geforce4 MX-440, TV-OUT** ■ Samsung SM-348B (48/24/16/48x) DVD/CD-RW Combo ■ Front-USB ■ LAN 10/100

Rechnerpreis:

€ 599,-

Art.: SEPGE2

Versandpreis: 581,03 EUR*

Die aufgeführte PC-Konfiguration versteht sich ohne Betriebsystem!

Wunsch-PCs

Konfigurieren Sie Ihren PC ganz nach Ihren Anforderungen und bestellen Sie ganz einfach Online in unserem Konfigurator. Wenn Sie möchten, bauen wir Ihnen Ihren Wunsch-PC für nur 20 Euro auch zusammen.

„Für die ganz Eiligen!“

Bei uns erhalten Sie Komplett-PCs bereits zusammengebaut ab 399,- Euro, oder Notebooks schon ab 999,- Euro – sofort zum Mitnehmen !

„Service für Alle“

Auch wenn Sie Ihren PC nicht bei uns gekauft haben, bieten wir Ihnen unseren fairen Service: wir rechnen zeitanteilig nach angefallenem Aufwand ab, maximal jedoch 1 Stunde !

Geschickt...

Wir liefern Ihnen Ihre Bestellung schon ab 5 Euro Versandkosten. 90% aller Lieferungen werden bereits innerhalb eines Werktages zugestellt !

www.atelco.de

■ *22 ATELCO-Filialen bundesweit* ■ *Online-Shop* ■ *Preisliste als Online-Flyer per e-Mail* ■ *Anmeldung und weitere Infos unter www.atelco.de*

ATELCO Computer

Seit über 10 Jahren!

* Hinweis: Bitte beachten Sie, dass der genannte Preis ausschließlich bei Versandzustellung und zzgl. Versandkosten gilt

Sicherheit total

Inkl. Firewall
und Anti Dialer

Panda Software

Kompletter Schutz für Ihre Daten

- *Maximaler Schutz gegen Gefahren aus dem Internet*
- *Automatische tägliche Aktualisierung*
- *Firewall Schutz gegen Hacker*
- *Installieren und Viren vergessen*
- *Anti Dialer*

Antivirus

Panda Software Deutschland
Wir gehen an Grenzen

www.panda-software.de · Tel. 02065/987-654